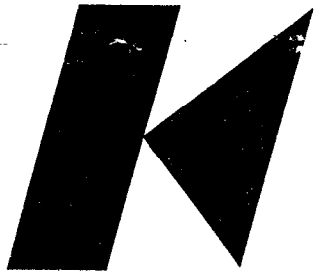
5879



**Contract HHS-100-91-0036**

# FINAL REPORT OF THE TASK FORCE ON THE PRIVACY OF PRIVATE-SECTOR HEALTH RECORDS

**KAI (KUNITZ and ASSOCIATES, INC.)**
6001 Montrose Road
Suite 920
Rockville, MD 20852

September 1995

KAI
Kunitz and Associates, Inc.

**FINAL REPORT OF THE TASK FORCE ON THE PRIVACY OF PRIVATE-SECTOR HEALTH RECORDS**

*TABLE OF CONTENTS*

## *PREFACE*

The Department of Health and Human Services (DHHS) Task Force on the Privacy of Private Sector Records was established in April of 1990 by Martin H. Gerry, then Assistant Secretary for Planning and Evaluation, in response to growing concern about the privacy of private sector health records as expressed by such senior level officials as Secretary Louis W. Sullivan and Dr. Bonnie Guiton, Special Advisor to the President for Consumer Affairs. Task Force members were drawn from the Department's major operation divisions as seen in the listing of Task Force Members that follows. Some turnover in membership occurred.

The Task Force's mandate was to examine the extent to which there were problems with the collection, storage, and use of health information in the private sector. Emerging events refocused the Task Force's mission to examining how to protect the privacy of all health care information within the context of health care reform and the developing electronic health information networks. This occurred first with the Sullivan plan for administrative simplification of billing and reimbursement, and later with the Clinton Administration's health care proposal. The Task Force examined existing needs for health care information, current laws and practice related to the privacy of health records, and steps the Federal government could appropriately take in protecting health records.

This Report first provides an overview of the Task Force's findings and recommendations. Findings are presented as answers to policy questions. Following sections provide materials that support these findings and recommendations and present a historical overview of events since the release of the Privacy Protection Commission's report in 1970.

To fulfill its mandate, the Task Force obtained information and advice from key participants in the health care sector through a series of meetings with representatives from the diverse community that develops and uses health information; through a conference on "Health Records: Social Needs and Personal Privacy"; and by an exhaustive literature review. A listing of those who advised the Task Force is presented in Appendix A. We gratefully acknowledge the importance of their contribution. Thanks are also due to Rene Kozloff and Michele Gargano for their efforts in preparing the Task Force report. Individual Task Force members also contributed their energy and expertise to preparation of this report. Special thanks are due to Joan Turek-Brezina, John Fanning, Richard Friedman, Johanna Bonnelycke and Willie Ethridge for their efforts.

The growing demands for health care information and the continuing move toward computer based patient records available over electronic networks will require ongoing dialogue on methods of protecting the confidentiality of health information. We hope this report will contribute to that dialogue.

Joan Turek-Brezina
Chair

## *SCOPE OF THE PROJECT*

The Department of Health and Human Services (DHHS) Task Force on the Privacy of Private-Sector Health Records was established in April, 1990 by Martin H. Gerry, then-Assistant Secretary for Planning and Evaluation, in response to growing concern about the privacy of private sector health records as expressed by such senior level officials as Secretary Louis W. Sullivan and Dr. Bonnie Guiton, Special Advisor to the President for Consumer Affairs. The Privacy Act of 1974 had addressed privacy and confidentiality concerns related to Federally held records. The Task Force's initial mandate was to examine the extent to which there were problems with the collection, storage, and use of health information in the private sector.

The Task Force was initially charged with:

- examining the extent to which there are problems with the use of personally identifiable medical and other health related records in the private sector;
- identifying what needs for health information exist in the public and private sector;
- reviewing current laws and practice related to the privacy of private sector health records;
- recommending steps that the Federal government could appropriately pursue to protect non-Federal record systems if problems were identified.'

Since its founding, emerging events refocused the Task Force's mission toward developing health care informationsystems, primarily electronic, in the context of health care reform. This divergence from the original mission occurred as first the Sullivan plan for administrative simplification of billing and reimbursement, and later the Clinton Administration's health care reform proposal were introduced.

This final report represents a summary of these efforts, and places them in the context of the other activities that have taken place prior to and coincident with them. It provides both a background and theoretical framework for addressing the issues and recommendations that emerged from the Task Force's efforts.

1. Mission Statement. Department of Health and Human Services Task Force on the Privacy of Private Sector Health Records. July 1991.

# HHS Task Force on the Privacy of Private-Sector Health Records

Joan Turek-Brezina, Chair
Office of the Assistant Secretary for Planning and Evaluation

Lois Alexander
Social Security Administration
(through May 1993)

A Prentice Barnes
Office of the Assistant Secretary for Management and Budget

Johanna Bonnelycke
Office of the Assistant Secretary for Health
(through January 1995)

Pat Brooks
Social Security Administration

Susan Callahan
Office of the General Counsel

Thomas Donnelly
Office of the Assistant Secretary for Public Affairs

Willie Etheridge
Administration for Children, Youth, and Families

John P. Fanning
Office of Health Planning and Evaluation

Richard Friedman
Office of the General Counsel

Thomas Hoyer
Health Care Financing Administration

W. Keith Lively
Office of the Assistant Secretary for Planning and Evaluation

Stanley Rosenfeld
Health Care Financing Administration
(through June 1993)

Harvey A. Schwartz
Agency for Health Care Policy and Research

Alan Wilder
Social Security Administration

Patricia Faley, Ex Oficio
United States Office of Consumer Affairs

*FINDINGS AND RECOMMENDATIONS*

As the nation examines options for reforming the health care system, policies must be in place to ensure that the privacy of health information contained in medical and other health related record systems is protected. The Task Force on the Privacy of Private Sector Health Records (The Task Force on Privacy) has explored the social, legal and economic issues affecting the privacy of persons who use the health care system.

The Task Force on Privacy was established in 1990 and charged with examining the extent to which there are problems with the use of personally identifiable medical and other health related records in the private sector. Emerging events, however, refocused the Task Force's mission to examining how to protect the privacy of all health care information within the context of health care reform and the developing electronic health information networks.

The Task Force examined existing needs for health care information, current laws and practice related to the privacy of health records, and steps the Federal government could appropriately take in protecting health records. Information was collected through meetings with representatives from the diverse community that develops and uses health information; through a conference on "Health Records: Social Needs and Personal Privacy" and by an exhaustive literature review.

Initially, to guide its inquiry, the Task Force identified a series of policy issues and questions to be answered in resolving these issues. The Task Force ultimately determined that eight major questions should be addressed before making recommendations about protecting the privacy of health records in future years:

- **What records should be governed by principles of health records privacy?**
- **Should "specially sensitive" records receive special treatment?**
- **At what level should legislation be enacted to protect health information?**
- **What constitutes informed consent for disclosure of health information and are there any circumstances under which informed consent may not be sufficient basis for disclosure?**
- **What is the impact of automation on the privacy of health records?**
- **What concerns are raised by the use of a unique identifier for health records?**
- **What type of structure is needed to oversee privacy policy, confidentiality and security matters and violations?**

- **What training, education, and awareness programs should there be for individuals regarding records containing information about them and for those working with health records?**

The following discussion summarizes the Task Force's response to these policy questions and presents its recommendations. Additional information related to these policy questions and a description of the events that have occurred since the release of the Privacy Protection Study Commission's report in the late 1970's are provided in the following sections.

*ANSWERING THE POLICY QUESTIONS*

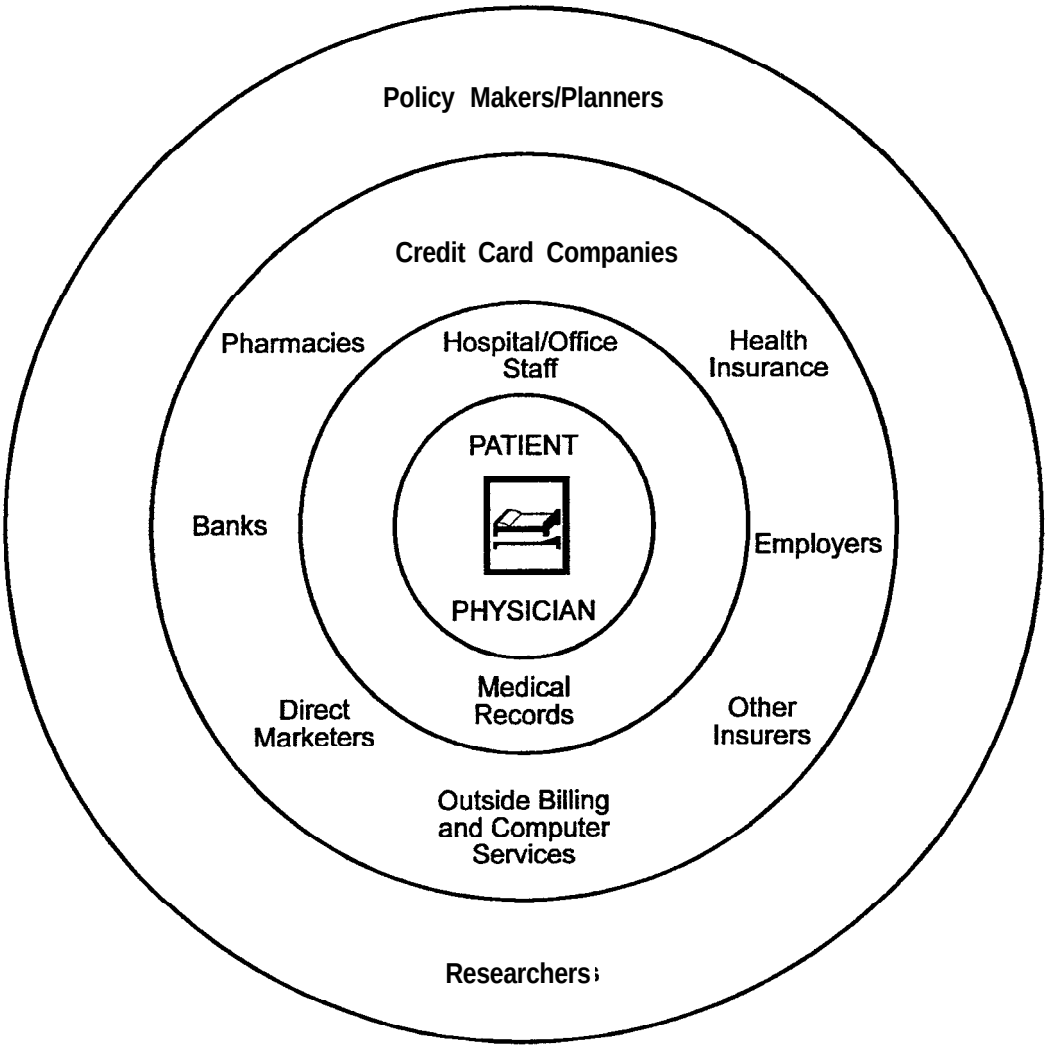
**What records should be governed by principles of health records privacy?**

Protecting individual privacy requires controlling access to health information. For this reason, the Task Force on Privacy examined the definitions of health records used by others and evaluated whether these definitions are still applicable in today's environment. In particular, the vast growth in the number of ways health information is used outside of the patient-physician relationship was taken into account when evaluating what health information should be included within the scope of protected records.

Information can originate within the health care system and be used by members of the health care team in the provision of health care and in the making of health related decisions for and about the individual. Information can originate within the health care system and flow outside of it for use by insurers, employers, pharmacies, and other institutions and organizations as shown in Figure 1. Information can also originate outside the health care system, either by self report or through investigation of an individual. For example, individuals are often asked about their health status or medical care when completing a new product warranty or redeeming a product coupon.

The Task Force questions whether any single definition of a health record would suffice in determining which health information should be protected either today or in the future. First, the kinds of records that contain health information are growing more numerous as health care is provided by and paid for in a variety of ways by a continually growing array of organizations and institutions.[1] Second, the automation of these records has the potential for making personal health information available to a wider audience through matching of individual units of information from many health and nonhealth sources to create new record systems. Third, health information is being collected and used more and more for nonhealth purposes.

# Figure 1:
# SPHERE OF ACCESS TO HEALTH RECORDS



Consequently, the Task Force believes that any file containing health information should be considered a candidate for protection since it is the information itself, and not the form in which it is maintained, which could result in an invasion of privacy if released. The Task Force also recognizes that it may not be possible to protect every item of health information. Clearly, information originating within the health care system and used in the provision of health care and in the making of health care related decisions for and about the individual should be protected. So should information that flows outside the health care system to insurers, employers, and other secondary users of data. However, sometimes information is provided by the individual in return for a service, such as in completing a new product warranty, redeeming a product coupon, or in becoming a preferred customer. The design of protections for information gathered this way is difficult because of the wide variety of potential collectors of information. Also, protection may appear less pressing than in the case of information provided in the course of actual medical care. How these emerging classes of health information ought to be protected needs to be addressed in light of future developments. In the meantime, individuals should be taught to be aware of the implications of any provision of health information, and to question organizations about the potential use of such information.

**Should "specially sensitive" records receive special treatment?**

The Task Force discussed at length whether particularly sensitive health records, such as those pertaining to diseases with social stigma or the records of socially or politically prominent persons, should receive special treatment or whether all records containing health and medical information should be considered sensitive.

Records that have historically been identified as sensitive contain information that has the possibility of injuring the data subject through public humiliation, stigmatization, loss of employment, insurance problems, or loss of the esteem of family and friends. Records containing information about alcohol and drug abuse, mental health, HIV/AIDS, sexually transmitted diseases, or genetic characteristics have been specifically identified as containing sensitive information.* However, other kinds of health records, less conventionally sensitive, also hold the possibility of injuring the data subject. For example, information on cancer or heart disease may be used in evaluating employment or loan decisions. There is also a growing consensus that much, if not all, health data provides information about genetic characteristics.

Although the Task Force agrees that it is appealing to classify information according to sensitivity, it questions whether this is the most effective approach to protecting data that may potentially cause harm to an individual. Disease-specific segregation of records necessitates complicated administrative arrangements since different requirements apply to different types of information. In addition, the definition of what constitutes a sensitive medical record may differ from decade to decade and from individual to individual. It may be more appropriate to determine what information individuals want released, under what circumstances, and to whom. For those who feel that all health data and records are sensitive

and should be protected equally, the very act of treating some records as specially sensitive implies that those containing "less sensitive data" are not being protected as well as they could be and implies that the data and the patient are less important. Common principles, rather than disease or subject specific ones, would better serve to protect all information.[3]

While protecting specially sensitive health records is essential to ensuring that the public has trust in the health care system and will supply accurate and timely information in the process of care, protecting *all* health records adequately is the issue that must be addressed.

**At what level should legislation be enacted to protect health information?**

The legal protection of health records is primarily a matter of State law. With the exception of substance abuse records, there is no general protection in Federal law for medical records. In the late 1970s, the Privacy Protection Study Commission recommended that "States retain their current role to regulate in conjunction with the creation or extension of a Federal role ".[4] They stated that the States should make the rules for all records other than Medicare and Medicaid and that State laws should provide enforceable expectations of confidentiality and patient access. The Commission further suggested that an outside body like the National Conference of Commissioners on Uniform State Laws develop model State statutes providing the rights recommended by the Commission. The Commission's decision to divide responsibility between the Federal government and the States was partially based on some hesitation about imposing rules by law or regulation on individual health care providers. However, the Commission envisioned that individual practitioners would eventually be covered by Federal requirements for data protection as it became necessary for them to qualify for Federal reimbursement either through expansion of existing Medicare and Medicaid regulations or through development of a national health care policy.

The Carter Administration sent a bill, the Federal Privacy of Medical Information Bill (1979-1980), to Congress that would have imposed medical record confidentiality obligations on all inpatient facilities regardless of Medicaid or Medicare connections. It would have also permitted the Secretary of Health, Education, and Welfare (HEW) to impose the rules by regulation on any outpatient facility receiving direct Federal funds under programs such as those offered by the Public Health Service Act. After Congressional consideration, the bill that was reported out by the House, and ultimately defeated, took essentially the same approach. There was little support for such a bill from the health care community.

At the same time, the American Psychiatric Association and the American Medical Record Association (now called the American Health Information Management Association) developed model confidentiality laws in the hopes of widespread State adoption. The National Conference of Commissioners on Uniform State Laws promulgated its Uniform Health Care Information Act in 1985, which to date has been adopted by two States. In 1979, the National Association of Insurance Commissioners promulgated a model insurance information privacy law, which has been the basis of legislation in several States. The usual format of such protective statutes is a statement that the information covered is confidential and may

only be disclosed with the individual's consent, or as provided for in the statute. The statute then sets out the exceptions, often with conditions. These statutes typically do not seek to control in any detailed way the collection of information; they assume that information will be collected. They therefore attempt to control its disclosure and to give the individual some say about its disclosure through consent processes.

Trends during the last decade have lead the Task Force, as well as many in the privacy and the health care communities, to reexamine the need for enactment of some form of Federal legislation covering all health records. During the 1980s, there was sustained growth in the amount of health information collected and the expectation of even greater growth to support the needs for information within a reformed health care system. There is also growing movement of health records across State lines due to the interstate nature of many health care businesses. Similarly, the American population is very mobile with significant movement across State lines. Finally, the growing importance of computer networks, including the move toward a "national network" being actively promoted by Vice President Gore, will make it significantly easier for health information to flow across State lines. Differing State law protections can both impair the flow of information from State to State, and leave the individual uncertain as to his or her rights and protections with respect to information. In addition, State law cannot control Federal access to information.

Recent efforts at crafting Federal legislation, as part of administrative simplification and health care reform, continued to focus on controlling access to information rather than on controlling the collection of information. These efforts often built on the recommendations of the 1973 advisory committee to the Secretary of Health Education and Welfare (HEW) in its report, *Records, Computers, and the Rights of Citizens.* The Secretary's Advisory Committee on Automated Personal Data Systems recommended that there be legislation establishing a Code of Fair Information Practice to apply to all automated personal data systems. The Code was to be based on fundamental principles of fair information practice, which the committee formulated this way:

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable data about him.

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.'

The Privacy Working Group of the Information Policy Committee, Information Infrastructure Task Force is now working toward applying these principles in new ways to reflect an era in which many records will be available in electronic form over a national network.[6] The general principles address information privacy, integrity, and quality. Principles for users of personal information describe the acquisition and use of data, and the need to give notice so that individuals can make informed decisions about releasing information. It addresses the need for protection of data, fairness in use of data, and the importance of education for users of data. Principles for individuals who provide personal information include a responsibility to understand the consequences of providing data to others and available redress if information is improperly disclosed or used.

While there is growing support for some form of Federal legislation, there is not as clear a consensus about the manner in which it would preempt State law. Federal law could set a uniform standard that all would have to follow, or it could establish a floor providing a minimum set of standards upon which State law could build. Those favoring a uniform standard are concerned that permitting States to establish additional protections will restrict the flow of information necessary for understanding and managing the health care system. Those who favor setting a floor argue that States, such as California, which have very strict protections should not have their current strong State protections weakened. During discussion of the Clinton Administration health care reform bill, consideration was given to establishing a floor, but limiting State choices for particular records that were considered vital to administering the reformed health care system.

**Under what circumstances should a record keeper be allowed to disclose an individual's health information?**

Disclosure of health information is restricted because of the fundamental principle of informational privacy -- individuals have a basic right to control the dissemination of private information about them. Although this right is overridden in circumstances where society's interests in disclosure outweigh the individual's right of privacy, the individual's right remains the starting point for any consideration of when disclosure of health information should be permitted.

The basic rule resulting from the informational privacy principle is that health information should not be disclosed without the individual's consent. The Task Force recognizes, as did the Privacy Protection Study Commission, that in many situations in our society, individuals are constrained to consent to disclosure of private information as a condition of gaining employment, insurance, medical care, or other necessary benefits. The Task Force concludes that most of the problems raised by such coerced consent must be dealt with

outside the context of privacy legislation; however, some of these problems can and should be addressed by requiring a consent form with specific elements in order to provide effective consent to disclose health information.

A consent form should be in writing, and should contain the following elements:

- subject signature;
- date of the signature;
- either a particular person or a category of persons who are authorized to disclose health information;
- the nature of the information that may be disclosed;
- either a particular recipient or a clearly defined category of permissible recipients;
- the purpose(s) for which the designated recipients are allowed to use the information, at the time of disclosure and in the future;
- an expiration date that is no more than one year away.

Such a form is necessary to give the individual a reasonable amount of information about the implications of the disclosure and to impose some reasonable constraints on the recipient.

There are circumstances where disclosure should be permitted even without the individual's consent. There are essentially four categories of such disclosures.

- Disclosure should be allowed without consent where it is necessary *to protect the individual's own health or safety.* However, this should apply only where it is not feasible to obtain the individual's consent.

- Disclosure without consent should be allowed *to protect the health or safety of another person.* This should be permitted only where there is a clear, substantial, and imminent danger to the health or safety, of one or more specific, identifiable individuals. Situations pitting individuals' interest in the privacy of their records against the health needs of other individuals are numerous and diverse, involving such difficult matters as genetic information and HIV test information. They must be resolved case by case, in light of the principle of "clear, substantial, and imminent danger to the health or safety, of one or more, specific, identifiable individuals. "

- Disclosures without consent should be allowed *for public health purposes*. Disclosure should be allowed to facilitate bioscientific and social scientific *research,* but only if the record keeper determines that any disclosure of individual identifiers is necessary for the research purpose, that any anticipated contact with the record subjects is necessary for the research purpose, that the research purpose is important enough to warrant any danger to individuals from such identification or contact, and that the recipient will have adequate

safeguards to protect the information. Disclosure ***to public health agencies*** should be allowed to help those agencies track diseases, assist persons who are afflicted or are at risk, and conduct research. Disclosure to ***institutions where the individual resides*** should be allowed within very narrow limits that severely restrict how the institution may use the information. In all of these situations, there must be strong limitations on redisclosure by the recipient.

- Certain ***miscellaneous*** disclosures should be allowed without consent. Disclosures should be allowed ***to auditing agencies or organizations*** who need records in order to provide accreditation or to review compliance with standards. Auditors should be prohibited, however, from using the information for other purposes. Disclosures should be allowed when ***pursuant to the legal process,*** but only when specifically ordered by a court, and only if the court determines that some substantive standard is met. This standard could involve balancing the individual's privacy interest, the interest in the particular disclosure, and any other general public interest in encouraging confidentiality. Also, in most situations, the individual should have notice of the legal process and the opportunity to oppose disclosure.

In all of these situations where disclosure is allowed without consent, there should be restrictions on how the recipient may use the information and prohibitions on redisclosure by the recipient.

**What is the impact of automation on the privacy of health records?**

Health records have existed in computerized form almost from the inception of computers. Traditionally, these records have supported specific functions, such as patient billing, rather than providing a comprehensive health profile of a specific individual. A dramatic shift, however, has begun that will radically change the individually identifiable information available in automated form. That is, we are moving toward development of comprehensive longitudinal computer based patient records available over a "national" electronic network.'

Recent attempts at administrative simplification or reform of the health care system have focused on development of sophisticated automated health information systems capable of providing comprehensive information about an individual. Such systems are viewed as essential to improving patient care. At the same time, there is not complete public comfort with this development. While acknowledging the benefits computers have brought to society, respondents to a 1993 survey conducted by Equifax[8] expressed concern about the dangers that the use of computers poses to personal privacy.

The development of electronic health care networks permitting standardized patient information to flow nationwide, and perhaps even worldwide, will require dramatic shifts both in how privacy is perceived and in how legislation protecting individual privacy is crafted. Traditional privacy protections were formulated around systems of records which

were in paper form or stored in centralized computer systems offering controlled access. The drastically different features of new automated systems must be taken into account when designing privacy protections. First, software systems are being developed that make it easier for users to combine and recombine bits of information rapidly by extracting data from a variety of sources. Thus, systems of records can no longer be viewed as relatively fixed entities. Where new record systems can be created almost instantaneously, the individual unit of health information becomes the basic construct around which privacy legislation must be crafted. Second, location has less meaning in an electronic world where records can be instantaneously available over information "superhighways". In the paper and pencil world, records were at a physical location, and access controlled by a single, easily identifiable entity.

The risks associated with an inadvertent release of information are much different in an electronic world where records can be accessed over national networks. As pointed out in the Institute of Medicine's study, *Computers at Risk: Safe Computing in an Information Age,* "society becomes more vulnerable to poor systems design, accidents that disable systems, and attacks on computer systems". At the same time, privacy protections can be more readily and effectively built into automated systems. Password protection and varying levels of access to data based on need to know, the sensitivity of the data, and the type of user can be readily implemented. Data can be released so that only the minimum amount needed to accomplish the task at hand is provided.

Establishing the proper legal framework that clearly prescribes who can access and share health information is critical to protection of this information in an automated world. It is easier to move records and more difficult for individuals to understand where information about them resides, by whom it is accessed, and for what purposes. Automation also makes it-more difficult for individuals to effectively control the redisclosure of information. In addition, as data can easily be transferred from setting to setting, questions of effective control by organizations are likely to arise. Legal protections must clarify what restrictions on the use of information apply to all entities which can call up identifiable information in automated systems; a clear framework eliminates this confusion. Finally, the introduction of cards carried by the individual to store significant amounts of information and to interface with computing systems will raise additional privacy concerns.

**What concerns are raised by the use of a unique identifier for health records?**

Automated systems now under development which provide comprehensive longitudinal information about an individual's health care will require some form of identifier which uniquely identifies the person who is the subject of the record. At this time, there are two major alternatives for this unique identifier: use the Social Security Number (SSN) or create an entirely new numbering system.

In the 1993 Equifax privacy survey which focused on health care, respondents recognized the need for such a unique identifier and the majority indicated their preference that it be the

SSN.[9] Those favoring use of the SSN argue that it provides the most cost effective and efficient approach. At the same time, the SSN has several shortcomings. The SSN is widely disseminated and used for a large variety of nonhealth related purposes, thus making it potentially possible to link health records with nonhealth related information. This potential ability to link many aspects of a person's life may, both in reality and in the perception of the public, facilitate the creation of dossiers about individuals. A health care number for every person developed especially for the health care system could just as easily become the basis for a national identification scheme, possibly a more efficient one than we have now. Thus, problems may be delayed, but not eliminated and possibly exacerbated, by use of a new system. To preclude broader usage, guidelines would have to be established prohibiting linkage of the SSN and a new identifier with each other and prohibiting use of the new identifier for linking health records with nonhealth records.

Developing a new number and restricting its use to the health care sector would ensure that each person's health number is of little use for linking health and nonhealth information. However, a new number may not be available for implementation within the titne frames envisioned for the development of automated systems and may be so costly to develop and implement as to be prohibitive. In addition, experience with the SSN suggests that initial restrictions on the use of a new, unique identifying number would be overridden in time in response to changing policy and public demands.

The SSN has certain technical limitations. There are people with more than one number and, less commonly, multiple users of a single number. It is also difficult to determine the validity of the SSN because there are no check digits or other security measures. Existing problems with the SSN would have to be corrected. At the same time, these features could be built into a new system. Many argue it would be cheaper to address the problems associated with the SSN than to create the bureaucracy needed to develop a new number.

**What type of structure is needed to oversee privacy policy, confidentiality and security matters and violations?**

The United States has not created any permanent oversight bodies in the data protection field. Such oversight bodies, which have been established by many European countries, perform a variety of functions such as giving expert advice, promoting fair information practices, receiving and investigating complaints, advancing and facilitating access rights, conducting systematic audits and investigations of particular information systems, and reporting periodically on problems and progress.[10] Some of these organizations are regulatory in nature while others rely on voluntary compliance. Proposals for a data protection authority started in the United States with the debate on the Privacy Act of 1974 and have appeared sporadically since, but they have received little serious attention.

Individuals now carry the burden for identifying improper data collection, data uses and users, and for resolving any problems. At present in the United States, perceived violations of personal privacy can only be addressed through litigation by an individual, a process that

is not only time consuming and prohibitively costly, but one that fails to identify the systemic problems and abuses that exist. A data protection authority would serve as the arbiter in data issues related to privacy and confidentiality.

Findings from the Equifax survey suggest that there is strong grass roots support for such an oversight body, especially for protection of health information. In the 1990 report *Customers in the Information Age,* Equifax asked respondents about privacy in general in a nationwide opinion survey conducted for them by Louis Harris and Associates and Dr. Alan Westin. The survey included interviews with 2,254 Americans, eighteen years and older, (public) and 916 corporate executives (leaders) from insurance companies, consumer credit grantors, banks and thrifts, direct marketing organizations, human resources firms, and consumer affairs companies. Respondents sampled in the public, and in the "leaders" group, were presented with three options for what is needed at the Federal level to protect consumer privacy:

- Stay with the present system of specific laws, congressional oversight and individual lawsuits;

- Create a nonregulatory privacy protection board to research and publicize new controversies over privacy for public policy considerations, and

- Create a regulatory privacy protection commission with powers to issue enforcement rules for businesses handling consumer information.

Results of the survey indicate that among the public, 41% believe a privacy commission with regulatory powers to enforce rules should be established, 24% think a nonregulatory privacy board would be beneficial and 3 1% think the country should stay with the same system. Corporate spokespersons who are consumer affairs executives were about evenly divided between the three options while the majority of executives in privacy intensive industries were in favor of keeping the same system--credit granters (55 %), human resources (5 1 %), insurance (49 %), banks and thrifts (43 %) and direct marketers (39 %).

In the 1993 Equifax survey cited earlier, a question was asked about the protection of health information within a reformed health care system. In this instance, there was stronger support for an oversight body. Eighty six percent of the public (1,000 respondents) and 69 % of "leaders" (651 respondents) supported creation of an "independent National Medical Privacy Board" to hold hearings, issue regulations, and enforce standards if national health care reform were enacted. The leaders interviewed include chief operating officers of hospitals, representatives of health maintenance organizations and health insurers, physicians, nurses, medical society heads, State regulators, State legislators, Congressional aides and human resources executives. These results are consistent with discussions between the Task Force and the wide array of organizations with whom meetings were held. While privacy advocates most strongly stated the need for a data protection board, others also saw a growing need for some type of oversight structure.

The success of the United States in competing in the international arena may well be related to its effectiveness in developing and implementing data privacy and security standards. At present, the U.S. lags behind other countries such as France, Germany, Sweden, and Canada in its national level data protection mechanisms. Data protection authorities have been in operation in other countries for more than a decade. Establishing such an authority would enhance the transborder exchange of personal information. [11]

Clearly, any move toward development of standardized, longitudinal health care records for individuals that are available over networks requires that policy attention be focused on protection of these records. Failure to do so could result in the public becoming less willing to provide the information on its health care and status that is needed for many socially important purposes. There has also been little or no debate about whether such an entity should focus solely on health care information or if it should be a larger entity that covers privacy issues more broadly.

**What training, education, and awareness programs should there be for individuals regarding records containing information about them and for those working with health records?**

Legal and technical requirements designed to protect the privacy of an individual are only as effective as those who implement and enforce them. Thus, education and training are integral m-maintaining confidentiality and privacy. Well developed, thoughtful programs need to be provided to those who are entrusted with private, personal health data and to individuals furnishing health information. Data handlers must understand their role and obligations in preventing fraud, abuse, breaches of confidentiality, and generally poor security practices. They should be taught feasible, effective practices to prevent such abuses.

Education can provide the public with information about individuals' personal rights or the responsibilities associated with furnishing data, and the consequences of consenting to the release of data. Campaigns are needed to heighten public understanding of personal and consumer rights and to promote an awareness of legal protections, violations of rights, and the redress available to an injured party. Because the concerns, interests, and practical issues of those who use data and those who furnish data differ, targeted programs must be developed for, and routinely provided to:

- health practitioners who provide direct patient care and collect data while providing medical services, usually on a one to one basis;
- people who provide health care support activities including health and life insurers, medical researchers, and hospital administrators who use this health information for payment for services, quality of care review, research, and administrative control;

- organizations and institutions which do not perform health related services, but collect personal health information in the course of everyday business, (i.e.; credit corporations, employers, educational institutions, etc.); and

- the public who provides and discloses personal data to the above organizations in the course of daily life.

Effective education and training programs for employees should:

- explain the legal requirements and responsibilities that employees who have access to health information possess with respect to data collection and disclosure;

- define terminology and concepts, review authorized and appropriate releases of data, and outline stipulations for penalties and sanctions for noncompliance;

- discuss the responsibilities and expectations of the employer, employee, and consumer; and

- provide the skills and tools needed to protect privacy and confidentiality.

Successful programs will provide each employee with a full understanding of the privacy and the civil rights of the persons about whom the data are collected, and should instill in them an appreciation of the significance of the data they are handling.

Consumer education programs should foster an arena of:

- personal privacy rights and health information, including the legal aspects of disclosure, access, and maintenance of personal data;

- methods to query organizations to access personal data, and how to review and correct erroneous information;

- persons who have the right to access or release personal data, and the legal and disclosure implications of informed consent; and

- steps of redress which may be pursued when personal privacy is violated.

For any consumer targeted effort to be successful, it is essential that the consumer understand what he or she is being told. Educational materials should be produced in various media, *i.e.;* written brochures, television ads, or radio spots, and must be made available in various "markets" appropriate to targeted socioeconomic groups and published in a variety of languages.

Many businesses have found that the costs of providing such programs are outweighed by the benefits of well informed and trained employees and educated consumers who are cognizant

of their rights." Education for the public and appropriate employees, whether provided by an institution, a State, or the Federal government, will help ensure that all concerned parties understand the possible ramifications of releasing health information maintained on individuals and the importance of confidentiality.

*RECOMMENDATIONS*

The Task Force on Privacy believes that the protection of health information is critical for the effective and efficient functioning of the health care system. It recommends that the following steps be taken to develop an effective and comprehensive privacy protection framework.

**Establish through Federal legislation national privacy standards covering all health records that (a) are based upon the basic principles of fair information practice enunciated in 1973, (b) treat all health records as specially sensitive, and (c) are appropriately preemptive of State laws.**

Federal legislation is needed to establish standards replacing the current patchwork of State laws and to protect records which increasingly are not confined by State boundaries. Federal legislation should cover all health information regardless of the system in which it is located. It is the release of information about an individual's health, rather than release of information from a particular record system, that has the potential for violating privacy. Records should be covered regardless of the form in which they are stored, their location, or the type of entity holding them.

The traditional principles of fair information practice enunciated in 1973 still offer a good guide to the protections such legislation should provide for individuals. People should know that information is being collected about them, and by whom it is maintained. They should be able to see and correct information about themselves. They should be informed of the intended uses and disclosures of information, and be offered an opportunity to prevent uses and disclosures not within those intended. Organizations creating, maintaining, using, or disseminating health information must assure the reliability of the data and take steps to prevent misuse.

The practical details of applying these principles to health care information in the form of legislation require careful attention, particularly in light of the massive developments in computing and telecommunications since the principles were drawn up. Likewise, other policy development activities, such as the "Principles for Providing and Using Personal Information" being developed by the Working Group on Privacy of the President's Information Infrastructure Task Force, will assist in applying the principles in the new technical environment. [13]

Legislation should clearly establish the requirements necessary for individuals to exercise informed judgement about providing information, or consenting to its release, including

delineating the rights of the individual, defining allowable disclosures by data collectors, and any instances in which information is not protected by Federal legislation, but is publicly accessible. A structure of penalties and a mechanism for enforcement should be developed and clearly defined.

All health information should be treated as sensitive and accorded strong protections, including assigning levels of access to particular kinds of health data on a need to know basis, and ensuring that informed consent has been obtained for release of the data. This will avoid the need to expand the definition of sensitive records if a new disease such as AIDS occurs, will account for differing individual perspectives on what information is sensitive, and will reduce the need for complex administrative systems. Records of politically or socially prominent people, or of employees of the data collection agency, may need to be accorded special treatment including the use of pseudonyms or encryption of identifying information.

Inherent in any proposal for Federal legislation is the preemption of the State's control, in some respect, over health information privacy. The existence of some very protective State statutes, and the increasing interest in nationwide uniform health record systems, present policy makers with a very serious dilemma. On the one hand, a weakening of existing privacy protection is hardly a good result of national legislation. On the other hand, lack of uniformity of law on this matter hinders efficient transfer of data across State lines, and makes it difficult to enforce protections. An approach to Federal and State legislation that retains existing strong protections while permitting necessary interstate data flow will enhance the utility of health data while allowing for its appropriate protection. Alternative methods of accomplishing this appeared in some confidentiality legislative proposals during the 103rd Congress.

**Establish a system of universal identifiers for the health care system.**

As the development of automated systems containing comprehensive, longitudinal information on individuals, accessible over national networks, continues, unique identifiers will be needed to help ensure the accuracy of information and the efficient operation of the health care system. It is important that this identification system not become a threat to personal privacy or the health care system itself. Ultimately, the real issue created by any number is the ability to easily match personal information across record systems. Although the Social Security Number is the most obvious candidate for a health care identifier, public concerns about the privacy implications of its use must be addressed. Its implementation must be accompanied by careful privacy protections that control the use and disclosure of information regardless of the identifier or linking mechanism.

**Establish effective security standards and guidance for health care information and foster a Federal leadership role in the development of security standards.**

Without effective security standards and guidance, the protections established in law cannot be effectively implemented. To ensure the effective flow of data, these standards must be national, or perhaps global, in scope. The current voluntary process for standards development should be fostered. However, it has not resulted in development of a comprehensive set of standards for the security of automated systems. The Federal government should assume a leadership role in the standards development process.

**Establish a data protection entity for overseeing and managing privacy and security.**

A data protection entity, by virtue of its oversight authority, would ensure that privacy goals are made visible and given importance. This entity would fill a major gap in America's privacy and security framework. Consideration needs to be given to whether a privacy entity should be established which only covers health care information or whether an entity covering all kinds of information is needed.

The focus of the data protection entity should be advocacy and research, not direct regulation. It should conduct a variety of activities including evaluating the development and implementation of privacy standards and guidelines, conducting research, studies and investigations, advising the President and Congress and others on the effectiveness of existing privacy policies, supporting the development of consent forms for the disclosure and redisclosure of information, offering leadership in the development of national standards for the security of information systems, and working with the health care community to foster educational efforts and the development of responsible privacy and security practices.

**Establish a comprehensive program fostering privacy and security education and awareness among all members of the health care community including consumers.**

Privacy regulations can only be as effective as those implementing them. Thus, all participants in all health care settings must be educated. The privacy protection authority should play an active role in the development of the necessary teaching materials for educating and training employers, employees, and consumers. This effort should include sensitizing Federal and private sector leaders to the issues of privacy and the ethical obligation to maintain confidentiality. In addition, large scale consumer education programs should be conducted to increase general awareness of the customary uses of health care information and the civil rights of the individual with respect to personal information and privacy.

## ENDNOTES


1. Amatayakul M, Wogan, MJ. ***Fundamental Considerations Related to the Institute of Medicine Patient Record Project.*** Paper prepared for the Institute of Medicine Committee on Improving the Patient Record. 1989.

***2.*** The Report of The Privacy Protection Study Commission. ***Record Keeping in the Medical-Care Relationship.*** July 1977:287.

***3.*** Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R, Steinauer DD. ***Privacy and Security of Health Care Information.*** Paper prepared for the President's Health Care Reform Task Force. June 1993.

***4.*** The Report of The Privacy Protection Study Cornmission, July 1977.

5. U.S. Department of Health and Human Services, Secretary's Advisory Committee on Automated Personal Data Systems. Washington, DC, 1973:41.

***6.*** Federal Register. January 20, 1995; 60(13).

***7.*** A variety of papers, articles, and books have addressed the development of comprehensive longitudinal computer-based patient records, including:

> Institute of Medicine. ***Health Data in the Information Age: Use, Disclosure, and Privacy.*** Donaldson MS and Lohr KN, editors. Washington DC. National Academy Press, 1994.
>
> Fitzmaurice M. ***Health Care and the NII.*** Rockville, MD. Agency for Health Care Policy and Research, June 1994. Publication. No. 94-0092.
>
> Schwartz HA. "Patient Care Data: Access, Privacy, and Use." Paper presented at the Tenth International Symposium on the Creation of Electronic Health Record Systems and Sixth Global Congress on Patient Cards, March 23-26, 1994, Washington, DC.

8. Louis Harris and Associates, Westin AF. ***Health Care Information Privacy: A survey of the Public and Leaders.*** Atlanta, GA: Equifax, Inc. 1993.

9. Louis Harris and Associates, 1993.

10. Flaherty DH. ***Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.*** Chapel Hill, NC: The University of North Carolina Press. 1989.

11. Rotenberg M, Culnan MJ, Rosenberg R. ***Computer Privacy and H. R. 3669, The Data Protection Act of 1990, Testimony Before the Subcommittee on Government Information, Justice, and Agriculture.*** Washington, DC: House Committee on Government Operations. May 16, 1990:17.

12. Christie L. Health Data and the Private Sector. ***Health Records: Social Needs and Personal Privacy.*** Presented at the DHHS Task Force on Privacy Conference, February 12, 1993; Washington, DC.

13. Working Group on Privacy. In process. ***Principles for Providing and Using Personal Information.*** Washington, DC: Author. 1995.

## *EVOLUTION IN THINKING SINCE THE LATE 1970'S*

### *INTRODUCTION*

Public concern and frustration with invasions of personal privacy surfaced in the late 1960's as anxiety over the growing use of computers emerged. The "discovery" of a large repository of personally identifiable data, which was being released without individuals' knowledge or consent, heightened the public's concern.' In response, a Department of Health, Education, and Welfare (HEW) Task Force (Secretary's Advisory Committee on Automated Data Systems) published a report in 1973, *Records, Computers, and the Rights of Citizens,** which proposed principles of "fair information practices" to govern the control, access, use and correction of record systems. The Privacy Act of 1974, designed to protect Federally held records, was an outgrowth this effort.

The Privacy Act also created the Privacy Protection Study Commission (PPSC, 1977) for the purpose of reviewing privacy standards, assessing needs, and developing effective and realistic recommendations for maintaining the privacy of all types of records. In laying the groundwork for its report, the Commission acknowledged a "growing public awareness and increased dialogue about the various dimensions of personal privacy. "[3] The Commission noted that, "in American society today, records mediate relationships between individuals and organizations and thus affect an individual more easily, more broadly, and often more unfairly than was possible in the past.. ." and it stated that this condition would remain true until "a proper balance between the individual's personal privacy interests and society's information needs" was achieved. In addition, the Commission found that while, "public opinion data suggest[ed] that most Americans treasure their personal privacy, both in the abstract and in their own daily lives, ... individuals are clearly also willing to give information about themselves, or allow others to do so, when they can see a concrete benefit to be gained by it. "[4] This situation remains true today.[5]

### *DEFINING A HEALTH RECORD*

In past years, health care was primarily a relationship between a person and his or her physician who developed and maintained information on the patient for his or her own use. Today, health care is provided by a growing number of health professionals and. institutions. Health information can also be found in the records held by pharmacies and laboratories, billing and computer services, credit bureaus, employers, research institutions, direct marketing companies, and Federal, State, and local government agencies. Insurance companies of all types maintain medical information as does the Medical Information Bureau, a database of medical information obtained primarily from applications for life insurance policies.[6] Other institutions such as correctional facilities, the armed forces, occupational health programs, and colleges and universities also maintain individually identified health care information.

Figure 1 presents an overview of the current spheres of access to health records.' Many of the records held by the organizations shown contain information in an individually identifiable form; that is, with the person's name, social security number and/or other identifier. Other records, for example, some of those used for research and statistics, may have individual identifiers attached at some stage, but not at others.

At present, there is no universally agreed upon definition for a health record. Previous examinations of the privacy of health care information have all provided definitions of a health record. The report of the Privacy Protection Study Commission classified health records into two categories: medical records and medical record information. They defined the ***medical record*** as a: "...record, file, document, or other written material relating to an individual's medical history, diagnosis, condition, treatment, or evaluation which is created or maintained by a medical-care provider." ***Medical record information*** was defined as: "...information obtained from a medical record or from the individual patient, his spouse, parent, or guardian, for the purpose of making a nonmedical decision about him. "[8]
The Commission focused on medical records and medical record information collected, maintained, used, and disseminated in individually identifiable form. It explored the ways in which this information was used in insurance, employment, public assistance, and social services records, and for research and statistics. The Commission noted that recorded information was used as part of a "gate keeping function" which determined "whether individuals should be allowed to enter into different types of social, economic, and political relationships, and if so, under what circumstances. "[9]

More recently, the Institute of Medicine Committee on Improving the Patient Record (Committee) issued a report on the Computer-based Patient Record, which built on the definitions proposed by the Privacy Protection Study Commission. They defined a ***patient record*** as "the repository of information about a single patient that is collected by health care professionals as a direct result of interaction with a patient or with individuals who have personal knowledge of the patient (or with both). "[10] It further distinguished a primary patient record used by "health care professionals while providing patient care services" from a secondary patient record which is "derived from the primary record and contains selected data elements to aid nonclinical users.. . in supporting, evaluating, or advancing patient care." The Committee definitions do not include health related data generated outside the health care system.

The Committee report's distinction between primary and secondary patient records is similar to Alan Westin's" approach to defining records. Dr. Westin points out that "...medical and health information has increasingly moved out of the offices of health care providers and into the record systems of a variety of non-providers. "[12] He identified three "zones" in which information is used: direct patient care activities (health care providers), supporting and administrative activities, and social uses of health data (secondary users). Zone 1 includes health care professionals and institutions who collect information in the process of providing medical care. Zone 2 focuses on the use of medical inforrnation for payment of services, quality control, and other administrative purposes. Westin also includes a third usage zone,

namely, the use of health information "for a wide range of social uses ranging from employment, life insurance, education and government licensing to civil and criminal judicial proceedings, rehabilitation and social welfare programs, public health investigations and reporting, medical and social research, law enforcement, and news reporting to the public. "[13]

*CONTEXT FOR EVOLUTION*

Concern with the privacy of health care records at the Federal level died down after an attempt to enact Federal legislation during the Carter Administration, *The Federal Privacy of Medical Information Act,"* failed. This bill received no Congressional support, reflecting the lack of support for Federal protection of medical information in general.

Renewed interest in the privacy of health information at the Federal level in the 1990's springs from several sources: the ongoing revolution in information technology and the move toward developing a national information superhighway, recent efforts at health care reform, the interstate nature of many sectors of the health care industry, and the growing inadequacy of State laws as more and more information moves across State lines. In addition, the number of records and the number of users accessing records has been steadily growing.

**Changes in Public Attitude Over Time**

In a 1970 survey conducted by Louis Harris and Associates, 34% of respondents answered "yes" when asked "Do you ever tend to feel that sometimes your sense of privacy is being invaded or not--that people are trying to find out things about you that are not any of their business". [15] By the early 1990's, concern with threats to personal privacy was widespread and remained at higher levels than in earlier Harris surveys.[16] In annual surveys they conducted during 1990, 1991 and 1992, respondents were asked "How concerned are you about threats to your personal privacy in America today--very concerned, somewhat concerned, not very concerned, or not concerned at all?" Between 78% and 79% of those interviewed said they were either very concerned or somewhat concerned about threats to privacy. In the 1978 Harris survey, only 64 % responded they were very concerned, or somewhat concerned, while 77% so responded in the 1983 survey.[17]

The 1990 survey also found that concern with threats to privacy was related to distrust of technology and the institutions of government and business.[18] Equifax's 1992 survey asked a series of questions about the use of computers to handle personal information. Although most respondents felt they had lost all control over how information about them is circulated and used by companies (71 %)[19], almost four out of five (79%) respondents agreed that computers had brought benefits to society and to them. At the same time, seventy six (76) percent agreed that "the present use of computers is an actual threat to personal privacy. "[20] In earlier surveys, Harris had asked respondents, "Do you feel that the present uses of computers are an actual threat to personal privacy in this country or not?"[21] Thirty-eight percent (38%) responded affirmatively in 1974, 41% in 1977, 54% in 1978 and 51% in 1983.

By the time of the 1990 Harris survey, the Privacy Act of 1974[22] had been in effect for approximately 15 years protecting records held by the Federal government, and had become known to much of the public. Perhaps as a result of this knowledge, when respondents were asked to react to a list of organizations which "collect and use information about people like you in a responsible way," responses indicated that they regarded governmental organizations as being more responsible than private industry in collecting and using personal information about individuals.[23]

In 1993, Harris interviewed health industry leaders and consumers on their attitudes regarding privacy issues associated with health information and health care reform.[24] They also conducted interviews with these leaders and consumers about general threats to privacy and the underlying sources of these concerns. The questions asked on earlier surveys were asked again. Earlier findings indicating widespread concern about threats to privacy continued with 80% of the respondents indicating they were "very" or "somewhat" concerned. Leaders in the health care field (78%) mirrored consumers in their concern about personal threats to privacy. It also appears that consumers were more distrustful of business, government, and technology than they had been in 1990.

More importantly, this survey provides the first direct information regarding attitudes toward the privacy of health information. Consumers, by a wide margin (85%), indicated that it is important to protect the confidentiality of medical information as part of any national health care reform.[25] Generally, consumers indicated that they trust those providing direct care to protect their medical records, with 87% of consumers expressing their belief that health providers keep medical information private. At the same time, they are worried about the wider circulation of health information. Forty-one percent (41%) expressed concern that medical claims information submitted under an employer health plan may be used in ways affecting their employment opportunities. Twenty seven percent of the consumers responding believe that an organization or person having medical information about them has disclosed it improperly. Of these, 31% believe they were harmed by the disclosure. About half of these consumers are concerned about the use of computers by direct care providers, while 75 % were concerned that computerized health information systems would be used for nonhealth care purposes. At the same time, consumers support societal uses of health information.

Even though 67% of consumers already believe strong laws exist protecting patient confidentiality, 56 % believe comprehensive Federal legislation should accompany any national health care reform. There was overwhelming agreement on what national legislation should look like:

> Ninety-six percent of the public believe any Federal legislation enacted should designate all personal medical information as sensitive and impose penalties for unauthorized disclosure. A similar 96% support rules spelling out who has access to medical records and what information can be obtained. Ninety-five percent favor legislating a right of access by individuals to their medical records in the system, and creating procedures for updating or correcting such

records. Finally 86% of the public favor creating an "independent National Medical Privacy Board to hold hearings, issue regulations, and enforce standards.[26]

Unlike other industries where leaders registered significantly less concern about privacy than consumers, health industry leaders scored similarly to consumers on privacy attitudes.[27] In general, consumers expressed higher levels of anxiety about computers and favored strong regulation, while leaders scored higher on controlling misuse of sensitive medical information and favoring strong privacy policies set by organizations handling medical information. In a question asked only of leaders, 50% indicated that increased computerization of records could be managed to help strengthen confidentiality while 45% indicated that computerization is almost certain to weaken confidentiality.

**Advocacy Groups and the Media**

As concern for privacy and confidentiality has grown, advocacy groups representing the public's interests and rights have played a key role in heightening awareness about the need to address emerging privacy issues. The popular press has also been increasingly reporting on violations of privacy and the public's response to such violations. Since the late 1980's, privacy advocates and advocacy groups have attempted to clarify the issues, voice public concerns, and promote remedies. Some groups advocate privacy efforts in general while others are targeting specific issues or groups. The Washington-based ***Privacy Times, the Privacy Journal,*** and the American Civil Liberties Union (ACLU) Privacy Project are all focusing on the impact of technology on access to information and individual privacy.[28] The White House Office of Consumer Affairs has played a leadership role in fostering a more general awareness of privacy issues. New groups have also been founded, many to address specific issues. For example, Computer Professionals for Social Responsibility (CPSR), and the United States Privacy Council, created by leading proponents of privacy in the United States, focus on privacy issues as they relate to computers.[29] The Privacy Clearinghouse, a public service funded by the California Public Utilities Commission, was established to foster telecommunications privacy for the State of California.[30]

Recently, there has been a marked increase in "privacy pieces" in the popular media. Members of the media have utilized all media forms to voice concerns, communicate the stories of "privacy victims, " and promote legislation and privacy efforts. The steady increase in media coverage over the last several years has contributed to the education of the consumer and to the raising of public awareness about privacy rights. The continued focus on privacy issues illustrates the concern for the safety of the individual and his/her personal health information. An electronic search of popular newspapers, magazines, and journals cited over 1,000 pieces written about privacy between 1988 and 1994.[31] These citations do not include the published journals of advocacy groups, or public or private organizations, corporations, professional, or trade associations. Televised vignettes and news stories about violations of privacy and security have also increased, reflecting and influencing national concerns.[32] Approximately half of these articles and programs were exposes of "privacy horror stories, " relating the circumstances, impacts, and repercussions of intentionally and

unintentionally disclosed data in hospitals, insurance and credit companies, private and public clinics. With the emergence of AIDS and advances in genetic testing, reporters have publicized stories of individuals' personal privacy violations related to this health information. Other major stories included the public's response to new uses and methods of access to personal information, advances in computers and telecommunications, and Federal, State, and local efforts to control and protect personal privacy. The Bibliography (Appendix C) contains citations for many of these articles.

*PRIVACY RELATED ACTIVITIES*

As individuals and organizations have become more aware of the need for significant improvements in the health information available for evaluating the effectiveness and efficiency of the health care system, there has been a growing tendency to establish organizations charged with examining, among other things, the need to protect health information. This section highlights the major efforts in the last few years and describes the kinds of activities they have undertaken.

**Committee on Improving the Patient Record**

The Committee on Improving the Patient Record (Committee) studied the feasibility and advantages of implementing a computer based patient record. Their final report (1991), entitled ***The Computer-based Patient Record: An Essential Technology for Health Care,*** recommended that, "health care professionals and organizations should adopt the computer-based patient record (CPR) as the standard for medical and all other records related to patient care."[33] The Committee envisioned a national health care information system with local, regional, and national networks in which patient records could be transmitted to any location where the patient was receiving care. "These networks would provide the means to transmit a laboratory report from a hospital to a physician's office or to send a patient record across the country."[34]

The Committee recognized the need for confidentiality protections. While it did not make specific recommendations about legal control over the computer based patient record, nor discuss the possibility of Federal legislation as a mechanism of control, it did recommend a review of Federal and State laws, and the promulgation of "model legislation and regulation to facilitate implementation and dissemination of the CPR.. ." Their report points to enactment of State level legislation with common elements across states:

> In order to protect the confidentiality of health records and to provide patients right of access to their health records and the right to include corrections to information in health records, all states should adopt uniform health care information legislation such as the Uniform Health-Care Information Act.[35]

**Computer-based Patient Record Institute**

One of the recommendations of the Committee was creation of the Computer-based Patient Record Institute (CPRI). Incorporated in 1992 as a membership organization, the CPFU

envisions a "comprehensive, longitudinal patient record to support all clinical, financial, and research activities. "[36] It is committed to promulgation of "uniform national standards for data and security to facilitate implementation of the computer-based patient record (CPR) and its secondary databases. "[37]

To meet its goals, CPRI has formed four work groups (CPR Systems Evaluation, Codes and Structure, Professional and Public Education, and Confidentiality and Privacy Legislation). The groups are focusing their efforts on standards development, systems evaluation, legal infrastructure formation, and public education. The Work Group on Confidentiality and Privacy Legislation is directing its efforts toward establishing the legal infrastructure to foster CPR implementation.[38] Specifically, this committee is responsible for examining the current state of legislation and for creating a more favorable environment for the deployment of CPRs and CPR systems. Finally, it has formulated statements on ethical, legal, privacy, and confidentiality issues to guide legislative activities initiated by the CPRI or its members. It has developed legislative language which has been submitted for consideration by the Board of Governors of the CPRI as model legislation.

**Administrative Simplification**

In November of 1991, then Secretary of Health and Human Services, Dr. Louis Sullivan convened a forum of national health care leaders to discuss the challenges of reducing administrative costs in the U.S. health care system. At the forum, health care industry led workgroups were created, including the Workgroup for Electronic Data Interchange (WEDI) and the WorkGroup on Computerization of Patient Records (WCPR). The **Workgroup on Electronic Data Interchange** looked at ways of increasing the use of electronic claims and examined the potential for uniform electronic billing. They recommended that Congress enact preemptive legislation governing confidentiality and ensure the uniform, confidential treatment of identifiable information in electronic environments.[39] The **Work Group on Computerization of Patient Records** looked at many of the same issues as the Comrnittee on Improving the Patient Record and supported the development of national standards for documenting and sharing patient information. They recommended that there be preemptive Federal legislation to resolve "inconsistencies and inadequacies in existing laws that protect patient privacy. "[40]

**Office of Technology Assessment**

Many of the health care reform proposals place substantial reliance on telecommunications and information technology to reduce costs and improve health care delivery. In. response to the growing interest in electronic records, the work of the Computer-based Patient Record Institute, and efforts to develop an information superhighway, the Office of Technology Assessment (OTA) of the United States Congress set out to examine the technology enabling the computerization and networking of medical information; identify privacy issues arising from computerization; examine the law dealing with privacy in medical information; and examine models and rules to protect privacy and determine whether new technologies can ensure privacy in the area of medical records.

In September 1993, OTA published a report, ***Protecting Privacy in Computerized Medical Information,*** that analyzes the implications of computerizing medical information and the challenges that it presents to individual privacy."' The report examines the nature of the privacy interest in health care information and the current state of the law protecting that information; the nature of the proposal to computerize health care information and the technologies available to both computerize and protect privacy; and models for protection of health care information. The analysis presented in the report reflects many of the same issues as those raised by the DHHS Privacy Task Force and explored at its conference, as well as concerns expressed by the public, privacy advocacy groups, and the other organizations that are addressing the influence of health care reform and automation on privacy and confidentiality.

**Information Infrastructure Task Force, Privacy Working Group**

The National Information Infrastructure (NII) is the web of communications networks, computers, data bases, and consumer electronics that will enable vast amounts of information to be available to large numbers of users. While private sector firms are developing and deploying that infrastructure, government will have a key leadership role in its development and in insuring that it is available to all Americans at reasonable cost. In undertaking development of the information infrastructure, the Clinton Administration is working closely with business, labor, academia, the public, Congress, and State and local government.[42]

The Information Infrastructure Task Force (IITF) was created by the Clinton Administration to articulate and implement the Administration's vision for the NII and to foster its development. The Task Force is made up of high level representatives of Federal agencies that are involved in the development and application of information technologies. They are working closely with the private sector to develop policies that will meet the needs of both the government agencies and the country. The IITF's goal is to foster the evolution of the National Information Infrastructure (NII) so that it may help the nation meet goals in key areas including: education and life long learning, libraries, health care, government services, environmental monitoring, manufacturing, and electronic commerce.[43]

The Information Policy Committee of the IITF, one of three working committees,[44] has created three working groups to address intellectual property rights, privacy, and government information. The Working Group on Privacy is charged with the "design (of) Administration policies to protect individual privacy despite the rapid increase in the collection, storage, and dissemination of personal data in electronic form" by providing guiding principles and making legislative and administrative recommendations.[45] In May 1994 the group published for public comment a set of principles for providing and using personal information, with the observation that "Traditional fair information practices, developed in an age of paper records, must be adapted to this new environment where information and communications are sent and received over networks on which users have very different capabilities, objectives, and perspectives. " The group continues to develop the principles in response to public comment. [46] The new principles are adapted to the advanced technology and communications of today and "recognize the changing roles of government and industry in information

collection and use. " Specifically, these new principles are intended to apply equally to private and government entities, increase the role and responsibility of data subjects, promote the reliability of the networks through which data will be travelling, and update the traditional and often obsolete ethics of privacy and create technologically appropriate rules of conduct."

Health Data Organizations

In early 1992, the Institute of Medicine, National Academy of Sciences, under a grant from the John A. Hartford Foundation, appointed the Committee on Regional Health Data Networks to examine issues and possible impediments to the effective use of regional health data networks. Their report, ***Health Data in the Information Age: Use, Disclosure and Privacy,*** focused on public release of descriptive and evaluative data on the costs and quality of health care institutions and providers and risks to,and protection of, the privacy and confidentiality of data that identify individuals in their role as patients or consumers.[48]

The Committee examined privacy, confidentiality, and security of information relating to individuals which it termed person identified (information such as an individual's name or DNA pattern permitting positive identification) or person identifiable (various items of information such as dates which when combined would permit identification) data. The Committee found that laws regarding data confidentiality (the disclosure or nondisclosure of information) are inconsistent and vary widely from State to State. Also, current laws offer little protection against redisclosure of an individual's health information; once a patient has consented to an initial disclosure (to obtain insurance reimbursement, for example), he or she has no way of knowing whether this information is being used for unrelated purposes without consent. They made three major recommendations regarding confidentiality and privacy of personal health data. The first, calling for preemptive legislation, recommends that the U.S. Congress enact legislation to establish a uniform requirement for the assurance of confidentiality for person identifiable health data and to specify a Code of Fair Health Information Practices that would ensure a proper balance among required disclosures, use of data, and patient privacy. This act would be enforced by the government, and penalties would be imposed for violations. A second recommendation calls for the establishment by health database organizations (HDOs) of an administrative unit or board to implement policies concerning protection of data and analyses; develop policies that protect the confidentiality of all person identifiable information consistent with relevant State and Federal law; develop educational materials for the general public that describe the rights and responsibilities of individuals and the protection given to their data by the organization; implement security practices in the data processing and storage systems of the organization; and implement an employee training program on the protection of person identifiable data. The Committee felt that although some organizations identify certain categories of data as being particularly sensitive, all data should be afforded stringent, and essentially equal, protection.

The Committee recognized that some person identified data, related to the processing of health insurance claims, must be released. However, the Committee recommended that a health database organization release this information only in the following circumstances: to other HDOs whose security protection is at least as stringent as their own; to individuals for information about themselves; to parents for information about a minor child; to legal representatives of incompetent patients; to researchers with approval from their institution's Institutional Review Board; to licensed practitioners treating patients in life threatening situations who are unable to consent; and to licensed practitioners treating patients in non-life-threatening situations, with the informed consent of the patient. The Committee particularly warned against allowing employers to require receipt of an individual's data from a health database organization as a condition for employment or the receipt of benefits. The Committee also studied the issue of a personal identifier for an individual's medical record. Although it felt that the Social Security number would be the obvious choice, it warned against its use on the grounds that the SSN offers too many opportunities to breach confidentiality and it called for a new unique identifier.

## *ENDNOTES*

1. The Medical Information Bureau (MIB) was established in the 1890's. Members of the MIB are life insurance companies who collect information from applications for life insurance completed by the applicant from consequent physicals and previous medical records. Data can be accessed by the MIB, member insurance companies, or the data subject, and can be used for ancillary purposes such as criminal and/or civil cases.

2. Secretary's Advisory Committee on Automated Data Systems. ***Records, Computers, and the Rights of Citizens.*** Washington, DC: Department of Health, Education, and Welfare. 1973. DHEW publication OS 73-94.

***3.*** Privacy Protection Study Commission. ***Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission.*** Washington, DC: U.S. Government Printing Office. 1977.

4. Privacy Protection Study Commission. 1977.

5. For a discussion of current public opinion on personal privacy and the confidentiality of health records see: Louis Harris and Associates. ***Health Care Information Privacy: A Survey of the Public and Leaders.*** Atlanta GA: Equifax, Inc. 1993.

6. Westin AF. ***Computers, Health Records, and Citizen Rights. New*** York: Petxocelli Books, Inc. 1977.

***7.*** Prepared by Task Force on the Privacy of Private Sector Health Records, Department of Health and Human Services. 1993.

***8.*** Privacy Protection Study Commission. 1977:278.

9. Privacy Protection Study Commission. 1977:281.

10. Dick RS, Steen EB, eds. The ***Computer-Based Patient Record: an Essential Technology for Health Care.*** Washington, DC: National Academy Press. 1991:11.

11. Alan Westin, LL.B., Ph.D, is a Professor of Law and Government, Columbia University. He serves as an academic advisor to Louis Harris and Associates and is a leading privacy expert.

12. Westin. 1977:7.

13. Louis Harris and Associates. 1993:9.

***14.*** H.R. 5935. ***Federal Privacy of Medical Information Bill. 1981.***

15. Westin AF, Baker MA. *Databanks in a Free Society: Computers. Record-Keeping, and Privacy. New* York: Quadrangle Books. 1972:466.

16. See: Louis Harris and Associates, Equifax, Inc. and Westin AF. The *Equifax Report on Consumers in the Information Age.* Atlanta, GA: Equifax Inc. 1990; and Louis Harris and Associates, Equifax, Inc, Westin A. *Harris-Equifax Consumer Privacy Survey 1992.* Atlanta, GA: Equifax Inc. 1992.

17. Louis Harris and Associates. 1990:1-2.

18. Louis Harris and Associates. 1990:4-6.

19. Louis Harris and Associates. 1992: 1.

*20.* Louis Harris and Associates. 1992:4.

21. Cited in Bennett CJ. *Regulating Privacy.* Ithaca, NY: Cornell University Press. 1992:39.

22. Privacy Act of 1974. 93-579 §5a1.

23. Trust in the Census Bureau (81%), the Social Security Administration (76%), and the Internal Revenue Service (67%) to protect privacy and confidentiality was generally greater than trust in private industry organizations. Sixty-eight percent of Americans had a high or moderate degree of trust in the way life insurance companies collect and use information, 67 % had a high or moderate degree of trust in health insurance companies, 65 % in companies which provide employers with information about job applicants and 34% in companies which sell to consumers at their home by direct mail or telephone. Louis Harris and Associates, Equifax Inc., Westin AF. *The Equifax Report on Consumers in the Information Age.* Atlanta, GA: Equifax Inc. 1990: VIII.

*24.* Louis Harris and Associates, Equifax, Inc. *Health Care Information Privacy: A Survey of the Public and Leaders.* Atlanta GA: Equifax, Inc. 1993. Study No. 934009.

*25.* Louis Harris and Associates. 1993:10-15.

*26.* Louis Harris and Associates. 1993: 11.

*27.* Louis Harris and Associates. 1993:19-20.

*28.* The *Privacy Times* is a bi-weekly journal edited and published by Evan Hendricks, founder of the journal. Mr. Hendricks has also authored a book entitled *Your Right to Privacy: A Basic Guide to Legal Rights in an Information Society.* The *Privacy Journal* is a journal edited and published by Robert Ellis-Smith. Also authored by him are the *Report on the Collection and Use of Social Security Numbers* and *War Stories: Accounts of Persons Victimized by Invasions of Privacy.* The ACLU's Project on Privacy and Technology was previously under the direction of Janlori Goldman.

29. United States Privacy Council. Information brochure. Washington, DC: Author. 1992.

30. Center for Public Interest Law. *Privacy Rights Clearinghouse, Mission Statement. San* Diego, CA: University of San Diego School of Law. 1992.

3 1. The publications reviewed include The *Washington Post, USA Today, New York Times, Wall Street Journal, Chicago Tribune, Los Angeles Times, Time, Newsweek, McCall s, Glamour* among others.

32. Televised programs which have spotlighted privacy include Nightline with Ted Koppel; ABC, CBS, and NBC Nightly News; Up Close with Maria Shriver and various daytime talk shows and news programs.

33. Dick. 1991:6.

34. Dick. 1991:51.

35. Waller AA. Legal aspects of computer-based patient records and record systems. In: Dick RS, Steen EB, eds. *The Computer-Based Patient Record: an Essential Technology for Health Care.* Washington, DC: National Academy Press. 1991: 177-178.

36. Computer-based Patient Record Institute. *An Imperative for Health Care: The Computer based Patient Record (CPR).* Chicago, IL: Author. 1993.

*37.* Dick. 1991:137.

38. Computer-based Patient Record Institute. *An Imperative for Health Care: The Computer based Patient Record (CPR).* Chicago, IL: Author. 1993.

39. Workgroup for Electronic Data Interchange Report to Secretary of U.S. Department of Health and Human Services, July 1992. See pages 16 and 17 for WEDI's discussion of federal-level legislation.

*40.* Work Group on Computerization of Patient Records. *Toward a National Health Information Infrastructure: Report of the Work Group on Computerization of Patient records to the Secretary of the U.S. Department of Health and Human Services.* Washington, DC: USDHHS. April 1993.

41. U. S. Congress, Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information.* Washington, DC: Government Printing Office. 1993. Pub.. No. OTA-TCT-576.

*42.* Information Infrastructure Task Force. The *National Information Infrastructure: Agenda for Action.* Washington, DC. September 15, 1993.

43. Information Infrastructure Task Force. ***Mission Statement.*** Washington, DC. September 15, 1993 and letter from Arati Prabhakar, Chair, Committee on Applications and Technology, Information Infrastructure Task Force, National Institutes of Standards and Technology, U. S.
Department of Commerce.

44. The three committees of the Information Infrastructure Task Force are the Telecommunications Policy Committee, Information Policy Committee, and Applications Committee.

45. The Information Infrastructure Task Force. *Executive* ***Summary.*** Washington, DC. September 1993.

***46. 59*** Fed. Reg. 27206 (May 25, 1994)

47. ***Preamble to Principles for Providing and Using Personal Information.*** Executive Office of the President. Washington, DC. April 1994.

***48.*** Institute of Medicine. ***Health Data in the*** *Information* ***Age: Use, Disclosure, and Privacy.*** Donaldson MS and Lohr KN, eds. Washington, DC: National Academy Press, 1994.

## *THE PROTECTION OF PARTICULARLY SENSITNE RECORDS*

### *INTRODUCTION*

Over the past two decades, there has been much discussion about "sensitive" health records, e.g., those identified as pertaining to diseases to which social stigma has been attached or to the records of socially or politically prominent persons, and whether they should receive special treatment. Stories abound about individuals who have lost employment, health and life insurance, social standing, family and friends, or who have been publicly embarrassed because of the release of sensitive health information.' This section discusses issues particular to such records.

### *INFORMATION PROPOSED FOR SPECIAL TREATMENT*

Records may be considered sensitive because of the disease or syndrome information they contain, because they belong to a particular person, or, according to many, simply because they contain *any* health or medical information at all. Records that have historically been considered as specially sensitive are those that society has viewed as containing information with a heightened potential for causing harm to the patient or data subject. Such information may also cause harm to others, such as the subject's spouse, children, friends, or sexual partners. The degree to which the information will cause public humiliation, stigmatization, lost employment, insurance problems, or loss of family and friends all contributes to it being identified as "sensitive. " For example, records containing information about alcohol and drug abuse, mental health, HIV/AIDS, sexually transmitted diseases, genetic characteristics, or adoption have generally been treated as sensitive. Records that contain information about socially or politically prominent persons have also been accorded special protections.[2]

In the early 1970's, the Privacy Protection Study Commission (PPSC) suggested that some medical records were more sensitive than others. The final report of the PPSC described the Federal statutes that had been enacted to govern the disclosure of medical record information related to alcohol and drug abuse, including the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970.[3] It also recognized the testimony given by the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) which argued that psychiatric records were particularly sensitive. In the end, the PPSC recommended the adoption of the Confidentiality of Alcohol and Drug Abuse Patient Records regulation[4] which proposed stringent requirements for maintenance of the confidentiality of alcohol and drug abuse patient records and the segregation of these records from general patient records.

The privacy issues posed by drug and alcohol abuse and mental illness[5] have resurfaced with the emergence of HIV/AIDS and genetic screening. There is concern that individuals will be less likely to divulge sensitive information about *sexually transmitted diseases, particularly* ***HIV/AIDS,*** *and genetic diseases* to health care providers if they are not assured that it will be kept confidential. As a result, persons at risk may not receive appropriate testing, counseling, or treatment to protect themselves and to protect the public health.[6] Failure to disclose a

communicable disease such as HIV/AIDS may pose a risk to the health of sexual or needle sharing partners.[7] In the past, the National Center for Health Statistics (NCHS) expressed concern that patients and/or physicians would not report sexually transmitted diseases, as required by State health departments, in order to protect the patient from social stigma, thereby resulting in unreliability of the data on the incidence of these diseases.*

Most States have addressed the special protection of HIV/AIDS records. A contagious disease among stigmatized or vulnerable groups, together with the availability of a blood test to identify persons who could transmit the disease but who were not overtly ill, raised complex and pressing questions.[9] Most States enacted laws addressing these issues. At the same time, there were calls for Federal legislation to protect the privacy of persons with the HIV infection, especially in order to induce people to be tested.

In response, Dr. Otis Bowen, a former Secretary of the Department of Health and Human Services, while not totally ruling out Federal legislation, stated that the responsibility for confidentiality law resided primarily with the States, and promised to work with the States to develop model legislation to protect confidentiality and prevent discrimination.[10] Shortly thereafter, in a letter to Governors, he called their attention to the National Conference of Commissioners on Uniform State Laws (NCCUSL) model law" which acknowledged the role of the States in protecting individual privacy while proposing the need for uniform State laws. [12]

The following year, the Presidential AIDS Commission on the Human Immunodeficiency Virus Epidemic recommended Federal HIV infection confidentiality legislation for the sake of confirming "our commitment to the principle of confidentiality in this epidemic, and to ensure national uniformity in confidentiality protection policies." At the same time, the Commission provided specific recommendations for the content of the Federal legislation and said that State model confidentiality legislation should be developed as a reinforcement to the Federal protection.[13] Congressional attention has continued, but there has been no legislation largely because of substantive disputes over what disclosures of information about persons with HIV infection should be allowed or required.[14]

Most States now have laws that address HIV-related information. About a dozen States have comprehensive schemes that address the confidentiality of such information in many settings. They identify allowable disclosures and impose restrictions on redisclosure.[15] The State of New York has probably the most rigorous HIV confidentiality statute in the country. It prohibits anyone "who obtains HIV-related information in the course of providing any health or social service or pursuant to a release of confidential HIV-related information, " from disclosing the data except in specific circumstances as set out in the statute.[16] The statute is a comprehensive scheme which addresses almost every conceivable reason for the disclosure of HIV-related medical information. For the most part, disclosure is authorized only when such disclosure is necessary for treatment of the affected individual, to prevent the use of infected body parts, for public health purposes, and for use by correctional agencies. The statute provides that "Confidential HIV-related information shall be recorded in the medical

record of the protected individual, " but does not require segregation of HIV-related information or the medical records in which it could be found."

Some State statutes (e.g. Oklahoma) define HIV-related information more broadly to include all HIV/AIDS related information held by any individual or organization.'* A majority of States, however, restrict coverage to a specific type of information (HIV test results), or to information held by certain agencies. [19]

***Genetic information,*** which indicates a predisposition for particular diseases/conditions, is generally considered to be sensitive because it has the ability to "stigmatize individuals, both in their own eyes and in the eyes of other individuals. "[20] Genetic information may also jeopardize a person's employment, life and health insurance, and/or social standing, even though having a "predisposition" does not mean a particular individual will actually experience the disease or condition. In addition, "the information affects other individuals--blood relatives of the individual tested, and living and unborn progeny. "[21]

Many people working in the field of genetic mapping, and especially those involved with the Human Genome Project, a joint effort between the National Institutes of Health and the Department of Energy, are aware of the social and ethical issues raised by the availability of genetic information. To this end, they have established the Committee on Ethical, Legal, and Social Implications (ELSI) to make recommendations for public policy.[22]

Under the authorizing legislation for the Human Genome Program, five percent of the appropriated funds must be devoted to studies of ethical, legal, and social issues.[23] The program has supported studies of the privacy and confidentiality issues created by the availability of genetic information. Interest in legislation regulating genetic information led to the introduction of a bill in the 102d Congress, and subsequently heard testimony on the need for a policy review of genetic screening and the use and protection of genetic information.[24] Testimony was given about individuals and their families having been denied employment opportunities, health and auto insurance, and the opportunity to adopt a child on the basis of the genetic makeup of family members.[25] Despite the efforts to categorize genetic information separately, there is some question as to whether, from the policy standpoint, it is possible to distinguish genetic information from other information about an individual, since many diseases are now understood as a complex mixture of genetic and nongenetic factors.[26]

The records of ***socially or politically prominent persons*** have also been viewed as requiring special protection to prevent the curious, or those who traffic, for profit, in information from gaining access to these records. Employees of an institution may be offered financial or other rewards for permitting unauthorized access to, or unauthorized disclosure of, medical information about socially or politically prominent persons, regardless of the sensitivity of the medical record. The disclosure of nothing more than the fact that a "celebrity" has been hospitalized, regardless of the cause, may be damaging in and of itself. Several hospitals that routinely admit "celebrities" as patients try to avoid the problem by assigning them

pseudonyms." The same desire to know about hospital admission and diagnosis applies to the records of a health care institution's employees and their relatives, friends, and neighbors.

*APPROACHES TO PROTECTING **SENSITIVE** RECORDS*

A variety of approaches have been proposed for protecting specially sensitive records including: segregating or separating the records; allowing different degrees or levels of access to records based on a "need to know"; requiring special consent before disclosing sensitive information; and/or developing legislation covering sensitive information. These approaches are often interdependent and interrelated. Although a more indepth discussion of legislative approaches to protecting health records is found in the section "Legislation to Protect Health Care Information," a brief discussion of legislation in relation to sensitive records follows.

**Administrative Safeguards and Automation**

Administrative approaches to protecting records include establishing procedures such as physically separating "sensitive" records from "nonsensitive" records, attaching pseudonyms to files, obtaining non-disclosure forms from employees, and assigning secure access levels. These approaches are valuable in that they can be customized to each institutions cultural, structural, and legal needs. Administrative approaches can work with existing paper systems and can also be effectively incorporated into automated systems.

Automation affords the opportunity to build procedures into electronic record systems for assuring that authorized access is permitted only to authorized persons for authorized purposes at authorized times. Computerized systems can be structured to assure that only the particular information necessary to a specific inquiry is shared. With paper systems, information is often provided a full page at a time. Privacy protection, including the protection of specially sensitive records, can be accomplished through password access, file access control, identity checking, and encryption and decryption, with a minimum amount of interference in the health care process.[28]

Automated records can also be segregated, with sensitive information being separately maintained and only accessible by specific authorization codes. Programs to link the sensitive information to the total patient record, where appropriate, would require the use of the special code, which may itself be confidential. As discussed above, some of the laws that exist to protect disease/syndrome specific records, such as those containing HIV/AIDS information, result in their segregation from other records in order to conform with statutory requirements.

Even if specific health information is not segregated from the rest of the health record, levels of access can be assigned on a need to know basis. Multi-tiered systems restrict access to information based on the user's access status. For example, the Indian Health Service, an agency of the U.S. Public Health Service, has developed, and is currently using, the

Resource and Patient Management System (RPMS) in several of its health care facilities.[29] The RPMS has been designed for multi-user access. One of its many excellent features is that specific data fields can be locked, thus permitting only authorized users to access them.

*PRACTICAL ISSUES OF SPECIAL TREATMENT FOR **SENSITIVE** RECORDS*

While many question how to classify information according to sensitivity, it may not be the most effective approach to protecting data that has the potential to cause harm to an individual. It may be more important to determine what data individuals will want released, under what circumstances, and to whom. Information can be effectively be kept separate in the process of health care delivery and prevented from "enter[ing] into the care-giving arena, patient files, and the mainstream of health information. "[30]

Developing policies for segregating sensitive from non-sensitive medical records depends on identifying what constitutes a sensitive medical record. There is little doubt that the disclosure to an employer or insurer of an HIV positive diagnosis may be harmful to the patient, regardless of the fact that many States have passed laws prohibiting the dismissal of employees or cancellation of health insurance because of AIDS or HIV infection. However, what constitutes sensitive information cannot be objectively defined and will be influenced by the individual's cultural values and beliefs. In addition, any health information whether it be "historically stigmatizing" or not, has the potential of influencing an employer's or creditor's opinions and decisions. For example, although cancer no longer carries quite the same stigma as in the past, knowledge that a potential employee or claimant has or has had cancer in the past may influence decisions concerning that person. For this reason, many have recommended that all records be treated as sensitive and protected from unconsented disclosure.

Disease-specific segregation of records has inherent limitations. It necessitates complicated administrative and management arrangements to maintain medical records, since different requirements will apply to different types of information - often information that logically belongs in the same record or file. The problem is not so serious if the segregation applies to specialized facilities, e.g., to drug and alcohol treatment facilities, or to special testing sites for HIV/AIDS, or for genetic information. It can, however, be serious when applied to medical care generally. Experience with the special confidentiality rules governing drug and alcohol abuse patients led to changes that eliminated the rules because they were unwieldy when providing care. Drug and alcohol treatment that is integrated with regular medical care is no longer covered by the special rules; these rules now apply only to specialized, separately identified, drug and alcohol treatment facilities or activities. In another instance,

drug and alcohol abuse and sickle-cell anemia patient records held by the Department of Veterans Affairs have long been subject to special confidentiality legislation, requiring a special consent form if the patient wishes to authorize disclosure. Congress recently added HIV-related information to this, and, in addition, forbade disclosure of the fact that a special written consent is required for such records to be disclosed. This presents a cumbersome administrative process that could be eliminated if the Department of Veterans Affairs required the special detailed consent form for all records, not just those covered by the special rules. [31]

With earlier interventions and some ameliorative treatments, the HIV infection is becoming a chronic disease for which patients will receive regular medical care over a long period of time, perhaps beginning with a test for HIV in a general medical care setting. Other aspects of that medical care will, in some instances, not produce "HIV-related information" or "HIV test results" as such, but the patient's status as being HIV infected will be a factor in the treatment, and other information in the record may demonstrate or suggest that the patient is infected with HIV. A strategy employing different sets of rules for different bits of information in what ought to be one record may not be the best way of managing records.[32]

*SUMMARY*

Those who believe that all health data and records are sensitive and should be protected equally argue that the very act of segregating records implies that those containing "less sensitive data" are not being protected as well as they could be and infer that the data and the patient are less important. Therefore, they believe that common standards, rather than disease or subject specific ones, should be developed to protect all information.[33]

While protecting specially sensitive health records is essential to ensuring that the public has trust in the health care system and will supply accurate and timely information in the process of care, protecting *all* health records adequately is the issue that must be addressed. A health care system, whether manual or automated, must ensure the completeness, accuracy, and integrity of all data, and must adequately protect all data from unauthorized access and disclosure.

## *ENDNOTES*


1. Smith RE, Siegel E. ***War Stories: Accounts of Persons Victimized by Invasions of Privacy.*** Providence, RI: Privacy Journal. 1990.

2. Privacy Protection Study Commission. Record keeping ***in the*** medical-care relationship. ***Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission.*** Washington, DC: Author. 1977:287.

***3. Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970,*** as amended by P.L.93-282, and the ***Drug Abuse and Treatment Act of 1972,*** amended by P.L.93-282.

***4. See 42*** CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records, ***Federal Register 52,*** 21796, June 9, 1987; Drug Abuse and Treatment Act of 1972 § 408, Pub. L. No. 92-255; Privacy Protection Study Commission. ***Final Recommendations of the Privacy Protection Study Commission.*** Washington, DC: Author. 1977; and Privacy Protection Study Commission. ***Personal Privacy in an Information Society.*** Washington, DC: U.S. Government Printing Office. 1977.

5. Britten G. ***Conference Overview.*** Presented at the DHHS Task Force on Privacy Conference, Health Records: Social Needs and Personal Privacy. Washington, DC. February 11-12, 1993.

***6.*** Gostin LO. Health Information Privacy. ***Cornell Law Review,*** pending publication. 1994.

***7.*** Gostin. 1994.

***8.*** National Center for Health Statistics. ***Health: United States 1975.*** Rockville, Maryland: Department of Health, Education, and Welfare. 1975: 3.

9. Fanning JP. HIV infection and the future of confidentiality policy. In ***Proceedings of the 1989 Public Health Conference on Records and Statistics. 1989: 161.***

10. Secretary Bowen. ***Testimony before the U.S. Congress, Subcommittee on Health and The Environment, Committee on Energy and Commerce.*** Washington, DC. September 21, 1987; and Press Release, U.S. Department of Health and Human Services. Sept. 23, 1987.

11. Letter, Otis R Bowen, M.D. to Governors, October 21, 1987.

12. National Conference of Commissioners on Uniform State Laws. ***Uniform Health Care Information Act.*** Minneapolis, MN: Author. 1985.

13. Report of the Presidential Commission on the Human Immunodeficiency Virus Epidemic. 1988: 126-128.

14. An analysis of the failure to enact confidentiality legislation appears in Prout DM. Congress blows its chance on AIDS confidentiality policy. *American College of Physicians Observer*. 1988;8(10): 12.

15. Fanning JP. *HIV Infection and the Future of Confidentiality Policy.* Presented at the Public Health Conference on Records and Statistics. Atlantic City, NJ. July 18, 1989.

16. NY Public Health s 2782.

17. See Intergovernmental Health Policy Project, The AIDS Policy Center. *Executive Summary and Analysis: Laws Governing Confidentiality of HIV-Related Information (1983-1988).* Washington, DC: George Washington University, for an analysis of other state statutes regulating the disclosure of HIV-related information.

18. Okla. Stat. tit. 63, sec. 1-502.22(A)(West 1985 & Supp. 1990).

19. See Iowa Code Ann. sec. 141.23 (West 1989) (covers HIV-related test information); Tex. Rev. Stat. Arm. art. 4419b-1, sec. 9.01(5)(Vernon 1987).

*20.* Yesley M. *Individual Rights and Expectations and Societal Needs.* Presented at the DHHS Task Force on Privacy Conference, Health Records: Social Needs and Personal Privacy. Washington, DC. February 11-12, 1993.

21. Yesley. 1993.

*22.* Wexler NS. *Hearing on the Protection of the Privacy of Medical and Genetic Information, Testimony before the U.S. Congress, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations.* Washington, DC. October 17, 1991.

*23.* Public Health Service Act § 485B, 42 U.S.C. 287c

*24. See* Conyers J. *Hearing on the Possible Uses and Misuses of Genetic Information, Testimony before the U.S. Congress, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations.* Washington, DC. October, 1991; and Conyers J. *Statement at Press Conference on the Human Genome Privacy Act.* September 13, 1990.

*25.* Transcripts of *Testimony Before the Subcommittee on Government Information, Justice, and Agriculture.* Washington, DC: House Committee on Government Operations. October 17, 1991.

*26.* NIH/DOE Working Group on Ethical, Legal, and Social Implications of Human Genome Research Genetic Information and Health Insurance. *Report of the Task Force on Genetic Information and Insurance.* May 10, 1993:8. Pre-publication copy.

27. Taken from a discussion at the Computer-Based Patient Record Institute, Workshop on Confidentiality, Privacy, and Legislation. Washington, DC. July 14, 1993.

28. Shneiderman B. ***Designing the User Interface: Strategies for Effective Human-Computer Interaction, Second Edition. New*** York, NY: Addison-Wesley Publishing Company. 1992:98.

29. Resource and Patient Management System. Indian Health Service, Office of Health Program Research and Development, ADP Systems Support Division. Tucson, AZ.

***30.*** Powers M. ***Consequences to the Individual: Data Collection, Information Use, and Electronic Health Systems.*** Presented at the DHHS Task Force on Privacy Conference, Health Records: Social Needs and Personal Privacy. Washington, DC. February 1 1- 12, 1993.

31. Farming JP. ***Confidentiality of Medical and Research Records.*** Washington, DC: U.S. Public Health Service. 1981.

***32.*** Fanning JP. ***HIV Infection and the Future of Confidentiality Policy.*** Remarks presented at the Public Health Conference on Records and Statistics. July 18, 1989; Atlantic City, NJ.

***33.*** Gostin LO. ***Individual Rights and Societal Needs.*** Presented at the DHHS Task Force on Privacy Conference, Health Records: Social Needs and Personal Privacy. Washington, DC. February 11-12, 1993.

## *LEGISLATION TO PROTECT HEALTH CARE INFORMATION*

### *INTRODUCTION*

This chapter discusses the status of legislation to protect health care information in the United States, the legislative developmental process since the 1970s, and some recent legislative proposals. It addresses continuing issues in choosing the appropriate level of government to provide statutory control over the use, collection, and disclosure of health care information and discusses the relative merits of State and Federal legislation.

### *BACKGROUND*

**Privacy as a Policy Issue: Inquiries and Legislation**

In 1973, an advisory committee to the Secretary of Health, Education and Welfare (HEW), in its report, ***Records, Computers, and the Rights of Citizens,*** recommended a code of fair information practices embodying policies to protect the privacy of persons whose records are maintained in automated systems. It included an "Action Agenda for the Secretary of Health, Education and Welfare, " which set out specific legislative and administrative steps the committee deemed necessary to carry out its recommended policies.' The committee recommended legislation "to establish a code of fair information practices for all automated data systems maintained by agencies of the Federal government or by organizations within reach of the authority of the Federal government. "[2] It recommended that the Secretary take administrative action to impose the requirements on "all systems that can be reached through grant, contract, or other relations with the Department. "[3] As the report did not address health care records specifically, these recommendations were presumed to apply to any type of record. The Committee's recommendation about the handling of research and statistical records was somewhat broader in scope. It specifically recommended preemptive Federal legislation to protect identifiable statistical research data from compulsory disclosure through the legal process, regardless of whether or not the data systems were supported by Federal funds.[4]

The Committee's recommendation for a code of fair information practices for Federal records systems found its fruition in the Privacy Act of 1974 which addressed data collection and maintenance by Federal agencies. It set up a comprehensive data management scheme and related procedures, including requirements for public announcement of Federal data systems, the right of individuals to see and correct their own records, and some restrictions on disclosure.[5]

The Privacy Protection Study Commission, established by the Privacy Act of 1974,[6] conducted a major study of data collection and use in the United States. In its 1977 Report, ***Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, the*** Commission encouraged the Federal government to take an active role in protecting medical records. The Commission felt that the most appropriate Federal role would build "on existing regulatory mechanisms and current certification and accreditation

processes, " and leave the basic protection to the States.' It recommended that the Social Security Act be amended to authorize the Secretary of HEW to require Medicaid and Medicare providers to "develop specific procedures" for implementing the substantive Commission recommendations with respect to disclosure of patient data and to patients' access to their own records. Compliance with this recommendation would, in the Commission's view, be a condition of participation in those Federal health care payment programs.

The Commission also recommended that States make the rules for all records other than those held by Medicare and Medicaid providers and that State laws should provide enforceable expectations of confidentiality and patient access. They suggested that an outside body like the National Conference of Commissioners on Uniform State Laws (NCCUSL) develop model State statutes providing the rights recommended by the Commission.[8]

The Commission's decision to divide responsibility between the Federal Government and the States was partially based on some hesitation about imposing rules by law or regulation on individual health care providers. Institutions were already subject to accreditation and certification processes to qualify for Medicaid and Medicare participation; individual practitioners were not. The Commission, however, envisioned that the requirements would eventually cover individual practitioners as part of the Federal mandate:

> Nonetheless, as it becomes necessary for private practitioners to qualify for Federal reimbursement, either through expansion of existing regulations, or through other developments looking toward a national health insurance scheme, they, too, would be covered by the recommended measures.[9]

The Commission's more general theory of the Federal and State roles in privacy protection is set out elsewhere in its report, and is based on "recognizing and encouraging the existing role of States." The specifics of protection take various forms, depending on whether the subject area is traditionally a matter of State regulation. In medical care, as in insurance, the Commission suggested "that the States retain their current role to regulate in conjunction with the creation or extension of a Federal role. "[10]

**Federal Legislation: Administration and Congressional Efforts**

In response to the recommendations of the Privacy Commission which appeared in July 1977, the Carter Administration set out to determine how to proceed with respect to the 162 detailed recommendations and the many other sentiments in the Commission's 600-page report.

The immediate contribution of the Department of Health, Education and Welfare, in October 1977, was a report to Congress endorsing the scope of coverage exactly as recommended by the Commission. The report indicated that the Department had considered and rejected coverage similar to that of the Federal drug and alcohol abuse patient confidentiality law. This law applied to records of any medical care activity conducted, regulated, or directly or

indirectly assisted by any Department or Agency of the United States." The Department concluded that such coverage would be "too sweeping for effective management and enforcement at the present time. "[12]

The bill that finally went to the Congress as part of the Carter Administration's program, the *Federal Privacy of Medical Information Act,*[13] took a slightly different approach. It applied directly to all inpatient facilities, regardless of Medicaid or Medicare connection. For outpatient facilities, it permitted the Secretary of HEW to impose the rules by regulation on any such facility receiving direct Federal funds under programs such as those authorized by the Public Health Service Act. It also included controls on Federal access to records held by all health care providers, whether or not the providers were covered by the obligations in the bill. After Congressional consideration of the Administration's proposal, the bill that was reported out by the House Government Operations Committee and considered by Congress (and ultimately defeated in a floor vote in the House) took essentially the same approach.[14]

In general, these policy efforts did not seek restructuring of societal expectations about collection and use of personal information, nor a decrease in the amount or types of personal information to be collected. The assumption was made that more and more data would be needed and used and that rules would be generated to see that the individual would not be harmed. The protections that were offered took a procedural approach, and paid little or no attention to privacy as an aspect of human dignity. While the protections aimed to assure that the individual would have a say in disclosure of information about himself or herself, there was little guidance on how organizations should decide what information an individual should be asked to disclose, or how individuals should decide whether to disclose information.[15]

**State Legislation: Developmental Activities**

The defeat of the Carter Administration's medical privacy initiative ended consideration of Federal level health record privacy legislation for some time and encouraged the ongoing interest on the part of some organizations in promoting State by State legislation. The American Medical Association and the American Hospital Association had opposed Federal legislation on the grounds that the States were addressing any problems that existed, and could continue to do so.[16] In addition, the American Civil Liberties Union and others were critical of the long list of disclosures of medical information that were authorized without patient consent. The AMA had earlier (June 1976) promulgated a model law for States to adopt and produced a revision in December 1981. [17]

At the same time, the American Psychiatric Association and the American Medical Record Association (now called the American Health Information Management Association (AHIMA)) developed model confidentiality laws in the hope of widespread State adoption." The National Conference of Comrnissioners on Uniform State Laws promulgated its Uniform Health Care Information Act in 1985 to apply to health information held by health care providers. To date, the Uniform Act has been adopted in two States, Montana and Washington. [19] The National Association of Insurance Commissioners (NAIC) promulgated, in 1979, a model insurance information privacy law which has been the basis for legislation

in several States. The model bill sets out provisions for notice of information practices, specifies the content of disclosure authorization forms, and provides for individuals' access to information about them. It also authorizes 17 separate disclosures without the written consent of the individual."

The usual format of such protective statutes is a statement that information covered is confidential, and may only be disclosed with the individual's consent, or as provided in the statute. The allowable disclosures without consent are then set forth, often with conditions that must be met before disclosure is made and conditions that must be met by those receiving the information. These statutes typically describe the conditions surrounding consent, and often give individuals a right to see and correct their records.

**State Law: The Present Situation**

Legal controls on the use and disclosure of personal health care information continue to be largely imposed by State law and the statutes generally follow the model described above. At this level, controls are found both in statutes and case law, but are neither uniform nor predictably protective across health care providers, settings, or States. A few States have comprehensive statutes reflecting systematic legislative attention to these issues.[21] State practice acts that license physicians, nurses, and other health care providers, and statutes that regulate health care facilities also contain provisions limiting unauthorized disclosure of patient information, although typically without much detail.** Most of these controls apply only to information held by health care providers. Information that is generated elsewhere or that migrates elsewhere is left to separate regulation or has no explicit statutory protection.

Some States have enacted statutes governing particular types of treatment information, such as mental health information[23] and HIV infection information.[24] These statutes differ greatly in the degree of protection they provide. Most States have statutory confidentiality protections for information that State health departments gather in their control of communicable disease.[25]

The vast majority of States have laws providing a physician-patient testimonial privilege for judicial proceedings, although its exact applicability differs substantially from State to State.[26] This is widely known, and is often perceived as an absolute confidentiality protection. In fact, it is of little practical importance in the management of health information since most instances in which health care information might be disclosed have nothing to do with judicial proceedings. Compelled disclosure is an important issue that is properly addressed by a privilege, but it is not common. The Privacy Protection Study Commission described it this way:

> The most important thing to remember about the testimonial privilege is that it has virtually nothing to do with normal, everyday use and disclosure of records maintained by a medical care provider. The discretion to disclose or not to disclose, in most circumstances, resides solely with the provider. The courts by and large uphold that autonomy.[27]

Direct Federal activities of all kinds (and some contract activities) are covered by the Privacy Act of 1974,[39] an information management statute with privacy protections that includes within its coverage records in Federal health facilities.

*THE RESPECTIVE ROLES OF STATE AND FEDERAL LEGISLATION*

Inherent in the discussion of Federal legislation is the notion of preempting States' control, in some respect, over health information privacy. The preemption of State laws by Federal regulation can, in general, occur in one of two ways.

- Absolute preemption would replace all State confidentiality laws with a Federal law. The Federal law would occupy the field of control of use and disclosure of health information, and States could not legislate in that area.

- What might be called "floor" preemption would allow States to make laws that are more protective of privacy than the Federal law. In the typical formulation of the latter approach, the Federal and State laws would be cumulative, and if either law forbade disclosure, the disclosure could not be made.[40]

In the case of absolute preemption, since States could not legislate regarding this subject, the Federal law would be the sole protection. The precise impact on the sum of privacy protections would of course depend on the content of the Federal law, but under many proposals it is quite possible that some protections now provided by State law would be lost. To the extent that States have imposed strict disclosure protections in areas like HIV/AIDS (on which almost every State has legislated),[41] and mental health records (the subject of detailed legislation in a few Sates), those protections would be eliminated if the Federal statute were not as protective.

The existence of some very protective State statutes, and the increasing interest in nationwide uniform health record systems, present policy makers with a serious dilemma. On one hand, a weakening of existing privacy protection is hardly a good result of national legislation. On the other hand, lack of uniformity of law on this matter hinders efficient transfer of data across State lines, and makes it difficult to enforce protections. A State specific approach to the protection of health information privacy does not reflect the realities of health care delivery and finance. State by State regulation will become more difficult as changes in the health care system make it possible for individuals to receive care anywhere in the country and for information for monitoring quality and cost effectiveness of care to be collected nationally. Health care providers, payors, and patients will be unable to make informed decisions about the use and dissemination of health information because there are no uniform regulations on which they can rely.[42]

A study by the Office of Technology Assessment noted the deficiencies of State by State regulation, stating:

There is an emerging" body of case law that imposes obligations on holders of health care information to disclose it only with care. Courts have based these obligations on various theories, including malpractice, contract, invasion of privacy, and a general public policy of confidentiality as evidenced by the physician-patient privilege and by medical practice acts that declare violations of confidentiality to be unethical conduct.[29] It is important to note that to the extent that a confidentiality statute governs governmental access to information, State law can control only the behavior of State officials. Federal compulsory legal process, for example, can force the disclosure of records regardless of whether State laws have forbidden disclosure. [30]

**Federal Law**

There is no general protection in Federal law for medical information. The one class of information that is Federally protected is records of substance abuse patients in facilities receiving Federal assistance.[31] This protection dates from the war on drugs of the 1970s, when a strong interest in inducing patients to seek treatment for drug abuse developed, with a concomitant recognition that confidentiality was important in that regard. The confidentiality protection was intended to assure individuals that they would not be harmed by inappropriate disclosure of information as a result of seeking treatment.[32] The legislative history of this section, as shown in the Conference Report, is clear as to its intent:

> . . .the strictest adherence to the provisions of this section is absolutely essential to the success of all drug abuse prevention programs. Every patient and former patient must be assured that his right to privacy will be protected. Without that assurance, fear of public disclosure of drug abuse or of records that will attach for life will discourage thousands from seeking the treatment they must have if this tragic national problem is to be overcome .[33]

The coverage of the statute is broad, applying to:

> . . .any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States.. ..[34]

Tax exempt status and tax deductibility of donations to an organization constitute Federal assistance, so as a practical matter all nonprofit drug and alcohol treatment facilities are covered.[35] The protection is not absolute. Some disclosures are permitted without patient consent, but they are carefully circumscribed, and the protection, is highly valued as "practical and effective Federal legislation" by the drug abuse treatment community.[36]

This is the only Federal statute approaching general applicability that protects health care records. Some health activities receiving Federal grant funding are subject to statutory confidentiality requirements as a condition of funding.[37] In other instances, grant statutes contain general directions to maintain confidentiality, but do not impose substantive requirements.[38]

> Legal and ethical principles currently available to guide the health care industry with respect to obligations to protect the confidentiality of patient information are inadequate to address privacy issues in a computerized environment that allows for intra- and interstate exchange of information for research, insurance, and patient care purposes .[43]

An approach to Federal and State legislation that retains existing strong protections, while permitting necessary interstate data flow will enhance the utility of health data while allowing for its appropriate protection. Alternative methods of accomplishing this appeared in some confidentiality legislative proposals during the 103d Congress.

## COMPUTERIZATION OFMEDICALRECORDS

Design of confidentiality legislation must now take into account the form in which records are used, stored, and transmitted. The speculations of the past about the possible impact of computerization on the use of records about people, and on privacy rights, were dramatically transformed in 1991 by a proposal that the United States move toward computerization of all health care records. A committee of the Institute of Medicine, in a report entitled The ***Computer-Based Patient Record: An Essential Technology for Health Care,*** recommended that:

> Health care professionals and organizations should adopt the computer based patient record (CPR) as the standard for medical and all other records related to patient care.[44]

The committee's detailed report discussed the virtues of moving toward a computer based record. One of the assumed virtues of any such system is the ease of transmitting patient records to any location where they are needed to care for the patient. The committee envisioned a national health care information system with local, regional, and national networks. "These networks would provide the means to transmit a laboratory report from a hospital to a physician's office or to send a patient record across the country. "[45]

The committee was aware of the need for careful confidentiality protections. While it did not make specific recommendations about legal control over the computer based patient record, it recommended review of Federal and State laws, and the promulgation of "model legislation and regulations to facilitate implementation and dissemination of the CPR.. ."[46]

An appendix to the Report prepared by a consultant discusses several legal issues relating to the record, including confidentiality. There is no discussion of the possibility of Federal legislation as a mechanism of control, and the conclusion points to State by State legislation:

> In order to protect the confidentiality of health records and to provide patients rights of access to their health records and the right to include corrections to information in

health records, all States should adopt uniform health care information legislation such as the Uniform Health Care Information Act.[47]

The specific question of whether Federal or State law is most appropriate for assuring protection for this new type of record was left to further implementation mechanisms that the committee recommended, like a Computer-based Patient Record Institute (CPRI), which has been established.[48]

*FEDERAL LEGISLATION: PROPOSALS, 1992-1993*

The efforts of the Administration and Congress to bring administrative simplification to health data exchange and to bring about major changes in the health care system produced proposals that would have imposed new confidentiality rules for health care information. They were not enacted, but offer interesting examples of solutions to some of the problems discussed above.

A 1992 Bush Administration proposal, ***The Medical and Health Insurance Information Reform Act of 1992***[49] was an effort to improve and make more efficient the health insurance system. It proposed an electronic network to carry information between health care providers and payers, in an attempt to reduce paperwork for patients and providers, reduce administrative costs and the difficulties associated with claims processing and adjudication and utilization review, provide physicians and health care institutions with clinical data, and provide consumers with information to compare the value of health care services.

The bill would have authorized the Secretary of Health and Human Services (HHS) "to promulgate requirements concerning health insurance information privacy and confidentiality protection for individuals. "[50] These requirements were to be based on the model State privacy protection act issued by the National Association of Insurance Commissioners. The requirements promulgated by the Secretary were to apply directly to administrators of self-insured employee plans. With respect to conventional insurance, the States would be expected to have State requirements applicable to insurers that were equivalent to the Secretary's standards. The requirements would also apply to Medicare hospitals with respect to electronic records they kept in compliance with other sections of the bill. Congress took no action on the proposal.

The Administration's efforts to simplify health data exchange also included task. forces and working groups, with representatives from the health care industry and professional organizations. They looked at ways of simplifying claims processing and computerizing records and concluded that Federal legislation was a necessity.

The **Workgroup on Electronic Data Interchange (WEDI)** was established in November 1991 as part of these inquiries. Its recommendations addressed many matters essential to simplification and uniformity, confidentiality requirements among them. WEDI recommended that Congress enact Federal preemptive legislation governing confidentiality,

and offered suggestions for the content, which were similar to, but less detailed than, earlier proposals for confidentiality legislation. Existing State disease reporting laws would be left in place, but apart from that the Federal law would govern use and disclosure of all identifiable health information in electronic environments. The group saw a central, Federal solution as necessary to protect the interests of patients, providers, and payors. The report called for special protection for especially sensitive records, but saw that as an element of the Federal legislation.[51] One of the significant features of the WED1 proposal was that it would apply only to providers and payers who collect, store, process, and transmit health care information in electronic *format.* Payers and providers who used paper records would continue to be bound by State laws and regulations. WED1 saw this as an incentive to ease the transition to automated transmission of health information.

Another study group conducting an inquiry in the same field, the **Work Group on Computerization of Patient Records,** also recommended Federal preemptive legislation. It approached its inquiry against the background of the Institute of Medicine Report, described above, and the desire to improve claims processing. Its recommendation that there be preemptive Federal legislation was based on the need "to resolve inconsistencies and inadequacies in existing laws that protect patient privacy. "[52]

*FEDERAL LEGISLATION: HEALTH CARE REFORM AND RELATED EFFORTS*

**The President's Proposal**

Efforts during the 103d Congress to establish new methods of paying for health care included significant proposals for information collection and related confidentiality protections.

The Clinton Administration's ***Health Security Act***[53] proposal was offered in November 1993 as a major restructuring of the way health care is paid for. It included significant proposals for collection of health data, and related confidentiality provisions. It called for protecting privacy while sharing information among the various proposed participants -- the National Health Board, health alliances, accountable health plans. The Act proposed various types of automation for data collection to provide higher quality, cost effective health care. The data collected would have provided information needed for quality assurance, analysis of practice patterns and patient outcomes, scientific research, and preparation of analyses to inform consumers of their health care choices.[54]

There were specific requirements for privacy protections for information created within the new system, as follows:

- The National Health Board would be required to promulgate standards for confidential treatment of individually identifiable information within the system, in compliance with the principles of the bill, in time for establishment of the system;[55]

- There would be sanctions and penalties for improper use of the health security card or unique identifying number;[56] and

- There would be ongoing monitoring of the system by a National Privacy and Health Data Advisory Council, composed of non-Federal personnel, including persons distinguished in the field of data protection and privacy and civil liberties and patient advocacy. [57]

Under this structure, individually identifiable data and personal privacy would have been protected by technical and administrative safeguards in conjunction with policies set forth in the bill:

- Disclosure would be carefully restricted to those uses authorized by the data subject, or for unauthorized, but predetermined and legally sanctioned purposes of operating the system or meeting criteria established by the NHB;

- Only the minimum data necessary to fulfill the need would be released;

- Each individual enrolled in the health plan would be able to access and correct his or her personal data;

- Each individual was guaranteed the right to know about data collection entities, what personal data is collected, and the uses of any collected data; and

- All data was to be transferred using only the unique identifier.'*

The bill would not interfere with the power of the courts to compel disclosure of patient information, or with State laws requiring reporting of communicable diseases, child abuse, or vital events.[59] It did not distinguish between paper and electronic records.

However, the bill did not address information outside the payment system. While it provided a basis for immediate substantive rules for information gathered in the new system, it did not cover other records, e.g., the clinical records of health care providers. For this class of health information, the National Health Board was required, within three years of enactment, to produce a detailed proposal for a comprehensive scheme of Federal legislation to protect privacy.[60]

**Comprehensive Privacy Legislation Proposal**

Rep. Gary Condit (D-CA), the Chairman of the Information, Justice, Transportation, and Agriculture Subcommittee of the House Government Operations Committee, initiated in 1993 an effort to draft legislation to protect the privacy of medical records without burdening the practice of medicine or increasing costs. He called together representatives from professional and industry groups to develop a consensus bill that would accommodate the diverse interests of patients, providers, insurers, researchers, Federal and State agencies and others.[61]

Confidentiality legislation proposed by the American Health Information Management Association formed part of the first working draft of the Condit bill.[62]

The bill that emerged was introduced as a free standing piece of legislation[63], but lent itself to being included in whatever piece of general health care reform legislation emerged. It sought to establish at once substantive confidentiality rules for health care information generally, without waiting for the proposal of the National Health Board, as proposed in the President's bill.

The Government Operations Committee included the bill's provisions, with modifications, in the President's Health Security Act, H.R. 3600 (which had been referred to the Government Operations Committee for consideration of the information and privacy provisions).[64] The bill did not distinguish between records maintained electronically and those maintained on paper.

The bill's treatment of State law displays an effort to resolve the tensions between nationwide simplification through preemption of State law and continuation of stronger State laws. The bill was preemptive with respect to State laws on matters other than disclosure (e.g. record keeping requirements, subject access). For disclosure restrictions, it was preemptive except with regard to disclosure restrictions for State laws "regarding public health or mental health". The effect was that stronger State laws in these areas, but not generally, would continue in effect. It left in place State laws regarding reporting of vital events and abuse of any person. For the Federal substance abuse confidentiality statute, it gave the Secretary of Health and Human Services power to choose the provisions of that law or the bill that provided greater protection.[65]

**Other Efforts**

Other legislation considered during the health care reform debate also sought to simplify transmittal and use of health data and to install nationwide health information privacy protections of general applicability.

Sen. Christopher S. Bond (R-MO), Sen. Donald W. Riegle (D-MI), Rep. David. L. Hobson (R-OH), and Rep. Thomas C. Sawyer (D-OH) offered the *Health Information Modernization and Security Act*[66], to facilitate establishment of a health data infrastructure, with Federal coordination to assist the private sector in developing standards. There were no substantive health information confidentiality rules included. The Federal panel that was to propose regulations for health information exchange generally was also to develop "requirements which protect the privacy of participants in the health care system and ensure the confidentiality of information in the data interchange system." The bills set forth principles, reflecting generally accepted data protection principles, that were to be taken into account in designing the requirements. [67]

Proposals for health care reform legislation in the Senate also included provisions for administrative simplification and related privacy controls. They followed closely the approach

of the bill introduced by Rep. Condit, but differed in some details. A Senate Finance Committee proposal was similar to the House Government Operations Committee version in its treatment of the relationship to State law,[68] as was a proposal by Senator Dole.[69]

No health record confidentiality bill was enacted during the 103d Congress.

*IMPLICATIONS FOR THE FUTURE*

Medical confidentiality legislation has traditionally been a State concern, with very limited exceptions. But changes in medical practice and in the ways information about patients is processed are the signals for a re-examination of the locus for legal control of tlhis information. Not very many years ago, medical practice was a local, even neighborly, affair. While gossip may have been a hazard, there was little occasion for the details of a person's health care to travel very far from the notes of the family physician, or the chart in a community hospital.

Recent developments in health care and its organization have changed this dramatically. The volume of useful medical information has increased, the medical care system has grown more complicated, more third parties are paying for care and want information about the care, and other sectors of society have seen the value to their own enterprises of health information about individuals. This has resulted in more detailed records, more people and institutions with routine access to them, and more demands to use them for purposes other than providing care.

More significantly, records are beginning to be used far from their place of origin as health care information is routinely crossing State lines. The electronic technologies currently in use and developing under explicit policy efforts toward computerizing all records, as well as organizational developments, will make the use of health care records an inherently interstate activity.

Both individuals receiving care and institutions providing or paying for care would benefit from uniformity in the rules governing use and disclosure of information. If patients are to understand and enforce their rights, they should be able to rely on a single set of rules. The advantages to institutions of major computerized record systems could be reduced by the need to comply with a variety of laws governing the use and disclosure of personal information.

These developments produced the widespread concern, the series of inquiries, and the attempts at legislation outlined above.[70] More hazards called for more controls, especially legal controls; but there was no clear answer as to whether those controls should be imposed by Federal law, or be left to the States in the hope that widespread adoption of a uniform law would provide effective protection. The attempt at Federal law failed. While several States have enacted comprehensive health record confidentiality laws, they differ; the model law of NCCUSL has been adopted in only two States.

Since then, the computerization of patient records has substantially modified the: concepts of *place* and ***record holder*** and probably made them ineffective as categories for defining controls over information. It has also affected the usefulness of State law as a mechanism of control. Even before widespread computerization, the possibility of records crossing State lines was cited as a rationale for centralized, uniform legal controls on use and disclosure of health information. Much of the motivation behind the 1979 and 1980 efforts at Federal legislation, and a uniform State law, was the need for uniformity so that, for example, persons who obtained their care in more than one State would know clearly and. readily what their rights were with respect to their records, regardless of where the records were held.[71]

## *ENDNOTES*

1. The Secretary's Advisory Committee on Automated Personal Data Systems, USDHEW. ***Records, Computers, and the Rights of Citizens.*** Washington: Author. 1973:136 et seq. US Department of Health, Education, and Welfare publication OS 73-94.

***2.*** The Secretary's Advisory Committee. 1973:136.

3. The Secretary's Advisory Committee. 1973:136.

4. The Secretary's Advisory Committee. 1973:102-103, 137.

***5.*** Pub. L. No. 93-579; the provisions applicable to Federal records are in 5 U.S.C. § 552a. See discussion of the history in Farming JP. ***Privacy as a Public Issue: History and Prospects.*** Presented to the Committee on Assessing Genetic Risks: Issues and Implications for Health, Institute of Medicine. September 17, 1992.

***6.*** The Secretary's Advisory Committee on Automated Personal Data Systems, 'USDHEW. ***Records, Computers, and the Rights of Citizens.*** Washington DC: Author. 1973:136 et seq. US Dept of Health, Education, and Welfare publication OS 73-94.6. Pub. L. No. 93-579, § 5.

***7.*** Privacy Protection Study Commission. ***Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission.*** Washington DC: Government Printing Office. 1977:293.

8. Privacy Protection Study Commission Report. 1977:93,94.

***9.*** Privacy Protection Study Commission Report. 1977:292.

10. Privacy Protection Study Commission Report. 1977:487-495; specific discussion of the health care issue at 491 and 493.

11. The present law, not substantially different, is discussed below at notes 31 and 32.

12. Letter, Joseph A. Califano, Jr., to Hon. Paul G. Rogers, Oct. 31, 1977, and accompanying documentation, ***Report and Recommendations on Statutory Protection for Health Records.***

13. Introduced as H.R. 3444 and S. 865 (identical), 96th Cong., 1st Sess., §310(2).

14. H.R. 5935, 96th Cong., 2d Sess. §101(8), as reported by the House Government Operations Committee. Discussion in H.R. Rep. No. 96-832, pt. 1, at 30-32 (1980). House floor consideration at 126 Cong. Rec. H31,207-31,222 and H31,288-31,299.

15. Fanning. 1992. There is a valuable discussion of this in Rule, J, ***The Politics of Privacy,*** 1980:69-72,114-124.

16. American Medical Association. ***Testimony before the U.S. Congress, Subcommittee on Health, House Committee on Ways and Means.*** 1980. (H.R. 5935, 96th Cong., 2d Sess. 61).

17. American Medical Association, Department of State Legislation, Division of Legislative Activities. ***Model State Legislation on Confidentiality of Health Care Information*** (as revised in 1981). Chicago, IL: Author. Undated. Earlier version is printed with the AMA statement, supra .

18. Prefatory Note, Uniform Health Care Information Act, 9 Part I U.L.A. 476 (1988).

19. Mont. Code Ann. §§ 50-16-501 to -553 (1993) and Wash. Rev. Code. Ann. §§ 70.02.005 to 70.02.904 (1992 and Supp. 1993-94).

***20.*** Trubow GB. ***Privacy Law and Practice. New*** York, NY: Bender. 1991:1987-1991. ¶ 8.04 [3] and [4] and ¶ 8.10.

21. Among the States that have comprehensive protections are Rhode Island (R.I. Gen. Laws §§ 5-37.3-l to -11 (1987 and Supp. 1994)); Maryland (Md. Health-Gen. Code Ann. §§ 4-301 to -309 (1994)); California (Cal. Civil Code § 56.10 to 56.16 (West 1982 and Supp. 1994)). Montana and Washington have enacted the Uniform Health Care Information Act of the National Conference of Commissioners on Uniform State Laws, discussed above. Wyoming has a comprehensive statute similar to the model law, but it applies only to hospitals. Wyo. Stat. Ann. §§ 35-2-605 to 35-2-617 (July 1994).

***22.*** Gostin LO. Health Information Privacy. Pending publication, Cornell Law Review. 1994:60.

***23.*** The District of Columbia and Illinois have such statutes. D.C. Code Ann. § 6-2001 to -2076 (1990 and Supp. 1994) and 740 111. Comp. Stat. Ann. 110/1-110/7 (1993 and Supp. 1994).

***24.*** There is probably no State that has not dealt in some way with use and disclosure of AIDS-related information. See Rowe M, Bridgham B. ***Executive Summary and Analysis: Laws Governing Confidentiality of HIV-related Information 1983-l 988,*** and ***Individual State Summaries: Laws Governing Confidentiality of HIV-related Information 1983-l 988.*** Washington DC: The George Washington University Intergovernmental Health Policy Project. This is out-of-date, but its citations provide a useful beginning for research.

25. Grad FP. ***Public Health Law Manual.*** 1990:284, with citations to representative State laws.

26. See Wigmore on Evidence §§ 2380 (1961 and Supp. 1991). See also, Gellman RM. Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy. ***North Carolina Law Review.*** 1984;62(2):255, ***272.***

***27.*** Privacy Protection Study Commission. 1977:284-285.

***28.*** In 1976 Alan Westin noted that there was no reported case in which a physician or hospital had to pay money damages for breach of confidentiality. Westin AF. ***Computers, Health Records, and Citizen Rights. New*** York: Petrocelli Books, Inc. 1977:26.

29. These theories and cases under them are outlined in Hall MA, ***Hospital am! Physician Disclosure of Information Concerning a Patient's Crime, 63*** U. Det. L. Rev ***144, 147-151*** (1985), and Annotation, 44 ALR4th 668.

***30.*** H.R. Rep. No. 832, 96th Cong., 2d Sess., pt. 1, at 30 (1980), and Gellman, op. cit., at 280.

***3***1. The protection is currently found in Public Health Service Act § 543, 42 U.S.C. § 290dd-2. Implementing regulations are at 42 C.F.R. pt.2.

***32.*** The protections first appeared in the Drug Abuse and Treatment Act of 1972 § 408, Pub. L. No. 92-255.

***33.*** H.R. Rep. No. 92-920, 92d Cong., 2d Sess. (1972), reprinted in 1972 U.S.C.C.A.N. 2062, 2072.

***34.*** Public Health Service Act § 543(a), 42 U.S.C. § 290dd-2(a).

***35. 42*** C.F.R. § 2.12(b)(4).

***36.*** Jacobs SL. Testimony of the Legal Action Center. Hearings before the Information, Justice, Transportation and Agriculture Subcommittee, House of Representatives, on The Fair Health Information Practices Act of 1994. May 5, 1994:431.

***37.*** For example, States which receive funds under the Public Health Service Act for sexually-transmitted disease activities are subject to a statutory command that they not disclose information obtained in connection with examination, care, or treatment of an individual without consent, except to provide service to the person, or as required by a law of a State or political subdivision. Public Health Service Act § 318(d)(5), 42 U.S.C. § 247c.

***38.*** For example, migrant and community health center grant recipients must have "organizational arrangements.. .for.. .maintaining the confidentiality of patient records". Public Health Service Act §§ 329(f)(3)(B)(ii) and 330(e)(3)(B)(ii), 42 U.S.C. §§ 254b(f)(3)(B)(ii) and 254c(e)(3)(B)(ii).

39. 5 U.S.C. § 552a.

*40*. This is the case with the Federal substance abuse confidentiality statute, Public Health Service Act § 543, 42 U.S.C. § 299dd-2, the regulation for which explicitly recognizes the effect of State law prohibiting disclosures which are permitted under the Federal statute. 42 C.F.R. § 2.20.

41. For a discussion of State confidentiality laws, see Gostin JD, Lazzarini Z, and Flaherty KM. Final Report: The U.S. Centers for Disease Control and Prevention; The Council of State and Territorial Epidemiologists; The Task Force for Child Survival and Development, Carter Presidential Center, 1995.

42. Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R, Steinauer DD. *Privacy and Security of* ***Health Care Information.*** Paper prepared for the President's Health Care Reform Task Force. June 2, 1993.

***43.*** Office of Technology Assessment, ***Protecting Privacy in Computerized Medical Information 44 (1993).***

***44.*** Dick RS, Steen EB, eds. The ***Computer-Based Patient Record, Institute of Medicine.*** Washington DC: National Academy Press. 1991:6.

***45.*** Dick. 1991:51.

***46.*** Dick. 1991.

***47.*** Waller AA. Legal aspects of computer-based patient records and record systems, in Dick. 1991: 178-78.

***48.*** Dick. 1991:148.

49. Introduced as S. 2878 and H.R. 5464 (identical), 102d Cong., 2d Sess.

***50.*** Proposed section 2211(a) of the Social Security Act.

51. Workgroup on Electronic Data Interchange. *Report to the* ***Secretary of U.S. Department of Health and Human Services.*** Washington, DC: Author. July 1992:15-17. More discussion and detail is found in Appendix 4: Confidentiality and Antitrust Issues, Technical Advisory Report.

***52.*** Work Group on Computerization of Patient Records. ***Toward a National Health Information Infrastructure: Report of the Work Group on Computerization*** ***of*** *Patient Records to the Secretary* ***of*** *the U.S. Department* ***of*** *Health and* ***Human*** *Services.* Washington DC: USDHHS. April 1993:26-27, Appendix D.

*53*. Introduced as H.R. 3600, 103d Cong., 1st Sess (1993).

54. The proposal is discussed at length in Hunter ND. ***Testimony before the U.S. Congress, Subcommittee on Technology and the Law, Committee on the Judiciary.*** Washington DC. January 27, 1994.

***55.*** § ***5120.***

***56.*** § ***5438.***

***57.*** § ***5140.***

***58.*** §5120(c) and Hunter. 1994.

***59.*** § ***5142.***

***60.*** § ***5122.***

61. Bureau of National Affairs. Rep. Condit launches effort to protect privacy of medical records. ***Health Care Electronic Data Report.*** May 12, 1993;1(1):12.

***62.*** The American Health Information Management Association's (AHIMA) proposed legislation (Draft Model Legislation, 8/11/93) addressed:

> the duty of the health care provider to protect the patient from undue intrusion and to safeguard the health information entrusted to him/her;
>
> confidentiality standards and penalties for violating these standards;
>
> standard policy describing user responsibility for confidentiality;
>
> education on confidentiality for all users of data;
>
> confidentiality agreements with all authorized users of data; and
>
> a policy for patient access to data.

The AHIMA proposal, while constituting preemptive Federal legislation, would have permitted states to continue to make confidentiality laws with respect to alcohol or drug abuse records and to psychiatric, psychological, mental health, or developmental disabilities health care records, and/or with respect to peer review or quality assurance records.

***63.*** H.R. 4077, 103d Cong., 2d Sess.

***64.*** H.R. Rep. No. 103-601, Part 5, 103d Cong., 2d Sess. (1994)

***65.*** § ***5194.***

66. S. 1494 and H.R. 3137 (identical) 103d Cong, 1st Sess. (1993). Bureau of National Affairs. Bipartisan effort takes aim at laying base for computer network. ***Health Care Electronic Data.*** September 29, 1993; 1(11):297.

67. § 2(a), amending Social Security Act, with confidentiality provision at § 2101(i)(5).

***68. S. 2351*** (as reported by Finance Committee, Aug. 2), 103d Cong., 2d Sess. § 402 (1994), adding a new subtitle C to title XI of the Social Security Act. Relationship to State law provisions at proposed Social Security Act § 11921.

***69. S. 2374,*** 103d Cong., 2d Sess. § 602 (1994), also adding a new subtitle C to title XI of the Social Security Act. Relationship to State law provisions at proposed Social Security Act § 11921.

***70.*** The Privacy Protection Study Commission discusses these developments in its report, p. 282. See also, Gellman, op. cit., supra note 7, p. 255. The problem, of course, was not limited to widespread dissemination of health records. The broad issue of designing protections in this changed environment is discussed thoughtfully in Rule, et al. ***The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New*** York, NY: Elsevier. 1980.

71. See Gellman, op. cit. at 280, and the Legislative Findings section of the Uniform Health Care Information Act, § l-101(5).

# DISCLOSURE OF HEALTH INFORMATION

## *INTRODUCTION*

Traditionally, privacy principles and privacy protection statutes have restricted disclosure of private information without the individual's consent. These restrictions are the most fundamental aspect of informational privacy.

This section will first discuss the nature of consent for disclosure of health information. What is the right to informational privacy that underlies disclosure restrictions? What are the traditional elements of informed consent to disclosure? What should a consent form contain and how should it be used? Are there situations where even a consent requirement does not give individuals meaningful protection? It will then discuss exceptions to the consent principle and when disclosure of health information should be allowed even without the individual's consent.

## *INFORMATIONAL PRIVACY AND CONSENT REQUIREMENTS*

### The Right to Informational Privacy

There are three basic underpinnings of the right of informational privacy.' One is the value our society places on individual autonomy: we safeguard informational privacy because we respect the individual's autonomous right to determine who shall know certain personal information about him or her. A second is the value we place on the individual self: we wish to create and foster individual personhood, and an individual's humanity is diminished when all his or her personal information becomes public property.

The third underpinning of the right to informational privacy is instrumental. In order to diagnose and treat illnesses, to perform research, or to perform epidemiological tracking of diseases, individuals must report health information to their physicians candidly and completely. If health information is subject to unconsented disclosure, individuals may report data inaccurately, incompletely, or possibly not at all; they may even be reluctant to seek treatment. Without assurances of confidentiality, the necessary candor and completeness would diminish or disappear.[2]

### The Need for Federal Statutory Protection

Eighteen years ago (1977), the Privacy Protection Study Commission recognized that the relationship between the patient and the health care provider must be confidential, and that this confidentiality must be guaranteed and enforceable. Specifically, the Commission recommended that:

> each medical care provider be considered to owe a duty of confidentiality to any individual who is the subject of a medical record it maintains, and that, therefore, no medical care provider should disclose, or be required to disclose, in individually identifiable form, any information about any such individual without the individual's explicit authorization ....[3]

The Commission did acknowledge that some exceptions to this consent requirement were appropriate, based on balancing the individual's personal privacy interest and society's need for information. Even with respect to these exceptions, the Commission recommended that the medical care provider be required to notify record subjects of the kinds of disclosures that could be made without consent.[4]

The Commission recommended that there be legally enforceable restrictions on disclosing most health records. It recommended that these restrictions be instituted by State statute, except that Federal regulations would continue to protect records on services covered by Medicare and Medicaid.[5] Now, eighteen years later, medical records are routinely communicated from State to State, and health care providers are anticipating development of a nationwide electronic network on which medical records would be accessed. For these reasons, it is essential to have consistent legal standards that would apply nationwide and to all medical records uniformly.

**The Elements of Informed Consent**

Legal, philosophical, regulatory, medical, and psychological literature have developed the concept of "informed consent" to define what kind of consent is required for a health care provider to administer a medical treatment to a patient. Informed consent is conceptualized as an "autonomous authorization" by the patient.[6] Authorization to disclose data is "autonomous" only if the patient understands the circumstances and implications of the proposed disclosure, decides to consent without control by others, and intentionally authorizes the process to begin.[7]

Two elements of this concept merit greater discussion. First, the consent must be *informed* -- *the* individual must receive enough explanation about the proposed disclosure, and must comprehend what he/she is told. Second, the individual must *consent* -- he or she must clearly manifest permission to disclose, and must act voluntarily.

**Information**

In order for an individual to give informed consent, he/she must have adequate information. The persons soliciting the consent must affirmatively provide a core set of information that is material in deciding to consent, and the individual must have the opportunity to obtain further information that he or she believes is important. Also, the individual must be able to comprehend the information.

The core information that must be given to the individual includes the purpose of the disclosure, to whom it will be made, during what period of time, how the data will be used, and the safeguards that are in place to protect the information.* These points are often contained in a consent form.

Individuals have different needs for information. Some may prefer only a brief notice; others may want a pamphlet describing possible disclosures; and still others may want to be able to call an 800 number for more extensive information.' Thus, there may be particular situations where one or more channels of information should be available beyond the core information provided on a consent form. An additional problem that merits consideration is that individuals may not realize what information they need, and may not know what questions to ask.

**Voluntariness of Consent**

Consent is fully voluntary only when the individual "acts without being under the control of another agent's influence."[10] The kind of influence that can compromise the "voluntariness" of consent occurs in several ways, including coercion, manipulation, or even persuasion. An individual may be coerced, as when consent is elicited by a threat of harm or force, or a threat to withhold a reward or benefit. An individual may be manipulated by presenting information in a way designed to influence him or her to do what the agent desires. At the extreme, the manipulation may involve lying, but it usually consists of omitting relevant information or presenting misleading information. In addition, there may be nonverbal manipulation by tone of voice or body language." Even nonmanipulative and non- coercive use of argument to persuade the individual to consent can, in some circumstances, be so forceful as to compromise voluntariness.

The most serious problem in ensuring that disclosure of health information is voluntary is coercion by threat of withholding necessary benefits. Routinely in our society, individuals are asked to agree to disclosure of health information as a condition of gaining or retaining employment, gaining admittance to a school, obtaining a license, or being considered eligible for services. In particular, individuals are compelled to give such consent in order to obtain health insurance. In theory, the individual can choose to withhold consent and forego these opportunities, but today's social, economic, and health structure make it difficult to do so.

The Privacy Protection Study Commission recognized these forces that tend to coerce consent. It also recognized that the users of health information form a web, such that information disclosed to one user tends to be redisclosed to successive other users. These concerns led the Commission to conclude that informed consent in its pure sense was not a practical standard -- when consent is a condition for obtaining necessary services, it is not wholly voluntary, and when the individual does not really know who all the ultimate recipients of the information are, and cannot accurately assess the costs and benefits of providing information, the consent is not fully informed.'* Although the Commission

concluded that "informed consent" in the pure sense was not practicable, it recommended what amounts to a modified form of informed consent -- a detailed consent form.

**Consent Forms**

A consent form should serve essentially two purposes. First, it should inform the individual of what will be done with his or her information, and/or why it will be done. Second, it should constrain the recipient of the information by limiting what the recipient can do with the information, to whom the recipient can disclose the information, or the period of time during which disclosure is allowed.

In practice, many consent forms are difficult to comprehend, often because they use technical and legal terms. Few consent forms identify the period of time for which the authorization is valid; many ask the subject to give consent for virtually an infiite time period. On many forms, the person requesting the consent does not justify his or her need for the data. Many are "blanket authorizations, " allowing dissemination of any and all identifiable information to the requestor, often without limiting the requestor's freedom to redisclose the information to others. Even more narrowly tailored authorizations often impose no constraints on redisclosure. Thus, patients consenting to disclosure of information to insurance companies may unwittingly be authorizing further dissemination of the data to direct marketers.

There have been attempts to develop a comprehensive consent form that is understandable and complete. *Statistics Canada* (Canada's central statistics agency) and the *Social Research and Demonstration Corporation* developed a form for use in a research survey. The form was four pages long, and was explained by an interviewer. It covered numerous topics, including the nature of the research; the confidentiality of the data collected; the record linkages to be undertaken; and the ways the records would be made anonymous.[13] Another proposal, by the *American Medical Record Association* (now the *American Health Information Management Association - AHIMA)* suggested that a consent form should include the following data: the name of the institution that will release the information; the name of the person that will receive information; the subject's name, address, and date of birth; the reason for the disclosure, or the recipient's need for the information; the extent or nature of the information to be released; the specific date, or condition upon which the authorization expires; a statement specifying whether the consent allows for re-release of the information at a later date; a statement that authorization can be revoked; the date the consent is signed; and the signature of the subject or legal representative.[14]

There is no consensus on how much information should be given. Giving individuals information about all reasonably likely primary and secondary uses of data would require very lengthy forms; a list of *all* potential disclosures would be impossible. Institutions soliciting consents have legitimate concerns that the very length and complexity of forms could induce individuals to withhold consent even though the disclosure would be worthwhile and would not damage the individual. In considering how much information to provide, it

would be helpful to conduct research to assess how much information an individual can absorb, comprehend, and apply in making a decision whether to consent to disclosure.

The Privacy Protection Study Commission's recommendation was that, where an individual's consent is required in order to disclose health information, that consent must be manifested in writing, in a document that meets the following criteria: (1) it must be signed; (2) it must state the date of the signature; (3) it must specify either a particular person or a category of persons who are authorized to disclose health information (4) it must specify the nature of the information that may be disclosed; (5) it must specify either a particular recipient or a clearly defined category of permissible recipients; (6) it must specify the purpose(s) for which the designated recipients are allowed to use the information, at the time of disclosure and in the future; (7) it must specify an expiration date that is no more than one year away (two years in connection with longer term health insurance policies)."

A requirement of this sort, as the Commission stated, ensures that the individual will have a certain level of information about the implications of the disclosure, without attempting to ensure that he or she fully understands every possible consequence of giving the consent.[16]

According to the Commission, if a consent form includes that set of information, and is written clearly and at an appropriate reading or comprehension level, it will serve its purposes. It will provide enough information to give the individual a functional understanding of the implications of the disclosure and also impose moderate constraint on the recipient.

**When Consent is Not Enough**

As the Privacy Protection Study Commission acknowledged, the practical reality is that consent for disclosure will often be given because of overwhelming pressures -- individuals will consent to disclosure of their health information as the price for obtaining necessary services or benefits. Even though it is impractical to attempt to forbid such practices, we should recognize that they constitute real dangers to privacy. There are three kinds of responses to these dangers.

First, there can be constraints on what constitutes valid consent, such as those suggested by the Commission. Such requirements would at least put individuals on notice of what information was being released, to whom it could go, and how it could be used.. Second, it may be appropriate to legislate to prevent certain persons' (employers, insurers) abilities to make certain decisions based on particular information. If an employer may not legally refuse to hire an applicant because of certain health conditions, the employer has less of an incentive to solicit information about such conditions. Such legislation would be outside of any privacy code. Finally, it may be appropriate to reorder social institutions to reduce or eliminate the incentive for disclosure. For example, if employers were freed of responsibility for paying health care costs for their employees, they would have less interest in obtaining

medical information about those employees. Here likewise, any legislation reordering these institutions would be outside the scope of a privacy code.

*EXCEPTIONS TO THE CONSENT REQUIREMENT*

The question of when a record keeper should be allowed to disclose health information without the consent of the individual is, basically, an issue of the limits of individual autonomy -- in what circumstances is the society justified in allowing, or even requiring, a disclosure of health information about an individual when he or she has not affirmatively consented, and may very well oppose it?

Permissible unconsented disclosures can be grouped into three categories: (1) disclosures to protect the individual's own health or safety; (2) disclosures to protect the health or safety of another person; and (3) disclosures for public health purposes. [17]

**Disclosures to Protect the Individual's Health or Safety**

Disclosure should be allowed without consent where it is necessary to protect the individual's own health or safety. A 1989 survey of State laws governing confidentiality of HIV information found that 12 States allowed unconsented disclosure when the individual's life or safety is threatened. [18] This would allow disclosure to a health care provider in am emergency when it is not feasible to obtain the individual's consent.

However, the law should not allow unconsented disclosure where obtaining consent is feasible -- to do so would unnecessarily override individual autonomy and intrude on the individual's sense of self and personhood. For example, the guidelines published by the American Hospital Association would not be sufficiently restrictive since they allow unconsented disclosure "in the event of direct referral or transfer of the patient to another medical care provider. "[19] The Privacy Protection Study Commission was also insufficiently restrictive in its recommendation to allow unconsented disclosure to a second health care provider when the individual is being referred to that provider for diagnosis or treatment.[20] There does not seem to be any reason why the first provider could not obtain the patient's affirmative consent to disclosure at the same time that it obtains the patient's consent for the referral itself.

**Disclosures to Protect the Health or Safety of Others**

Disclosure should also be allowed where necessary to protect another person's health or safety. However, a great many situations can plausibly be represented as meriting disclosure to protect other individuals' health or safety. To ensure that this exception does not swallow the rule of requiring consent, this exception should be limited to situations where there is a clear, substantial, and imminent danger to the health or safety of one or more identifiable individuals.

Thus, some State laws allow the disclosure of highly sensitive HIV test results to the spouse, sexual partner, or needle sharing partner of an HIV test subject;[21] to health care providers, crime victims, or law enforcement personnel who were exposed to infection;[22] and to a health care provider when necessary to provide care to the individual's child.[23]

In certain situations, it may be difficult to determine whether the danger to the other person warrants the invasion of privacy. One such situation occurs when genetic testing reveals that a person carries a gene for a trait that could affect other members of the person.'s family. Such a situation raises the question of when it is proper to break physician patient confidentiality to inform possibly affected individuals.[24] For example, if a person is a carrier for Tay-Sachs disease but has not revealed this to his or her spouse, should the doctor inform the spouse so that the spouse can be tested?

Another such situation is the HIV positive health care worker. There has been sharp dispute whether the possibility of transmitting HIV from an infected health care worker to a patient is great enough to require telling patients that the worker is HIV positive. The American Medical Association and the American Dental Association have advised HIV positive providers to inform patients of this status.[25] On the other hand, the former Surgeon General points out that the principle of informed consent requires advising the patient about reasonable risks, and that the risk of transmission from health care worker to patient is very low.[26] Also, public knowledge that a doctor is HIV positive can devastate his livelihood.[27] These factors militate against such a requirement in this area.

Even more serious problems would be raised by a disclosure to the individual's employer. An employer can normally obtain the employee's consent for reasonable disclosures; there is no reason to permit disclosure to an employer without consent, unless one of the other exceptions would apply.

Such situations will have to be addressed case by case; this report does not attempt to resolve particular situations.

**Disclosures to Protect the Public Health**

Disclosures for public health purposes include several disparate kinds of releases, among them disclosures to researchers, to public health agencies, and to managers of institutions where the data subjects reside.

**Disclosures for Research**

The term research includes not only academic and governmental scientists performing pure research, but also investigations performed by commercial firms. It includes social science as well as bioscience.

Disclosures for scientific and medical research or for statistical purposes can be divided into two groups, one more invasive into the privacy of the individual than the other.. Research that will entail contacting the individual, examining him or her, or contacting some other person in a way that will reveal health information about the individual is different from a statistical or epidemiological project that will analyze large numbers of medical records but does not need individual identifiers. The former kind of research involves activities that have direct effects on specific individuals, and that focus attention on those individuals' medical conditions; the latter kind of research generally has no such effects.

There is also an intermediate case. An increasingly important kind of medical research involves linking information from two or more separate data sets, either to form a longitudinal health care record, or to compare different kinds of information such as health care and income status. While this kind of research does not have direct effects on specific individuals, it often requires obtaining access to health information with identifiers attached so that the data from one set can be linked with the corresponding data in the other set.[28]

A statute should allow unconsented disclosures for research purposes, but should establish criteria for such disclosures. The criteria should be substantially more restrictive where the research entails individual contact or other activity that has a direct effect on the individual.[29] The statute should allow the disclosure only if the record keeper determines that each of the following tests is met: (1) if the disclosure is to include identifiers, disclosure of identifiers is necessary for the research purpose; (2) if the researcher is to contact the individual, such contact is necessary for the research purpose; (3) the research purpose is important enough to warrant the danger to individuals from additional exposure and from any subsequent contact; (4) the recipient will have adequate safeguards to protect the information, including any appropriate process to remove identifiers, destroy identifiers, or destroy records. [30]

The following additional protections may also be appropriate for disclosures for research purposes. First, personally identifiable patient health information, once linked with other personal information for research and statistical purposes, should never be used to take any action affecting the rights, benefits, or privileges of an individual patient. Second, the recipient must have security measures to protect the information from any unauthorized redisclosure. Third, researchers receiving identifiable data should not be allowed to redisclose, under the same penalties applicable to any other improper disclosure.[31]

**Disclosures to Public Health Agencies**

Reporting of health information to governmental public health agencies is a long established kind of disclosure. The 1989 HIV study found that at least 27 States had provisions for such reporting in statutes specifically pertaining to HIV and AIDS, and that this was the most common kind of provision allowing disclosure.[32] Such disclosure for both HIV/AIDS and other specified diseases allows agencies to track the progress of epidemics, to counsel and

treat persons who are at risk, and to conduct research. In general, such disclosures should be permitted without consent. However, this should be permitted only if there are strong legal and institutional safeguards against redisclosure by the public health agency. Also, it may be that for certain conditions (such as HIV infection), the disclosures to the agency should be with consent only, or should be made under pseudonyms, in order to avoid discouraging individuals from being tested and treated.[33]

**Disclosures to Residential Institutions**

Finally, there are disclosures without consent to the officials in charge of an institution where the individual resides. Such institutions include the prison where an individual is incarcerated, and the school that the individual attends.[34] The 1989 study found that seven States allowed disclosure of HIV information to corrections facilities, and seven. States had provisions allowing disclosure, sometimes with restrictions, to schools.

This kind of disclosure raises substantial problems. Any such provision needs to be considered very carefully and must be accompanied by strong restrictions on how the institution may use the information and who in the institution may have access to it. Residents can be greatly harmed by disclosing health information.

**Miscellaneous Disclosures**

A statute should also make provisions for disclosures to auditors and disclosures pursuant to legal process.

**Disclosures to Auditors**

A record keeper can have a legitimate need to disclose identified health information to auditors or reviewers who provide accreditation for the record keeper or for some aspect of its operations, or who review compliance with standards. Examples include the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) and peer review organizations. A statute should allow such disclosures without consent only if the auditing function requires access to information with identifiers. Also, the statute should prohibit the auditor from using the information for any purpose not directly related to the auditing function, and in particular for any purpose that would harm the individual. The statute should prohibit the auditor from redisclosing any such information in reasonably identifiable form. Finally, it should require the auditor to maintain an accounting of the disclosure.[35]

**Disclosures Pursuant to the Legal Process**

Disclosures pursuant to legal process includes disclosures in response to subpoenas, discovery,[36] and court orders. An important problem is that State and Federal law typically do not recognize any substantive right of the individual to have his or her health. information kept confidential. Nor does the law typically give the individual any procedural right to have notice of any attempt to obtain health information from the record keeper, or to oppose the attempt before any tribunal. The recordkeeper does have some substantive and procedural

rights, but it can resist disclosure only by expending substantial time, energy, and money (on legal fees), and it often has little or no self interest in opposing the disclosure. Thus, if a law merely allows the recordkeeper to resist disclosure, it does not afford adequate protection; the law must either **oblige the** recordkeeper to resist disclosure or else afford the individual some substantive and procedural rights.[37]

The substantive protection that the statute should afford is that unconsented disclosure should be allowed only where it is determined that a particular standard is met. Certain State statutes allowing disclosure of HIV information under court order provide good models. These statutes allow disclosure only if the court finds that there is a compelling need for the information and that the need cannot be otherwise accommodated. Also, the statutes require the court to consider the individual's privacy and to consider the public health interest against allowing a disclosure that might deter individuals from being tested.[38]

The major procedural protection that the statute should afford is that the determination discussed above should be made by a court. Disclosure without consent should require an order by a judge, not merely a subpoena or discovery request; the court is a neutral arbiter that can take into consideration the individual's privacy interests.[39] Also, to ensure the most objective and serious consideration, the exception should be limited to orders of a court, and should not extend to orders of an administrative tribunal.

There should be further procedural protections. Where possible, the individual rnust have notice of the legal process, and must have the opportunity to oppose disclosure."' A pseudonym should be substituted for the individual's real name in any publicly accessible court files, and the court should conduct the proceedings in chambers unless the individual consents or the court finds that the public interest requires an open hearing.

**Limitation on Redisclosure**

If society does authorize certain disclosures of health information without consent, it must consider how to limit the resulting harm to the individual -- the incursion on his or her autonomy and the diminution of his or her personhood. The best means of limiting these effects are by restricting the recipient's freedom to redisclose the information and by limiting the uses to which the recipient can put the information. Such restrictions are necessary when the individual is identified in the information or is reasonably identifiable from the information.

Recipients who routinely collect, store, or use such health information should be governed by exactly the same set of requirements as the original recordkeeper. This would be the case for health care providers, insurers, and researchers. Because these types of people are accustomed to handling and protecting health information, and because they often commingle the received information with the other health information they collect, it is necessary, and

not unduly burdensome, to require them to treat this information the same way they treat the other health information they collect.

However, where the recipient does not routinely collect and store such information, and especially where he or she would normally commingle this information with entirely different kinds of information, the law allowing the recordkeeper to disclose health infonmation to this recipient should include a specific prohibition on further disclosure, and it should require the recordkeeper to explicitly recite this prohibition at the time of the disclosure.

*SUMMARY*

Individuals have a right to restrict disclosure of information about them. To effectuate this right, there should be a basic presumption, enforceable by law, that health information about an individual must not be disclosed in reasonably identifiable form without his or her consent. The legal protection for this right should be in Federal statute.

Consent to disclosure should be manifested in writing. In order to give the individual a reasonable amount of information about the implications of the disclosure, and in order to impose reasonable constraints on the recipient, the consent form should meet certain requirements. It should specify, clearly and comprehensibly, who may disclose information, what information may be disclosed, who may receive it, and for what purposes the recipients may use it. The consent should also have a time limit after which it expires.

There are circumstances where the law should permit disclosure of health information even without the individual's consent. One is where it is necessary to protect the individual's own health or safety, and obtaining consent is not feasible. A second is where there is a clear, substantial, and imminent danger to another person's health or safety. A third category of situations are those where disclosure furthers public health; this category in particular requires close attention to whether disclosure in identifiable form is necessary. Disclosure should be allowed pursuant to legal process, but only when specifically ordered by a court, and only where the court determines that there is a compelling need that outweighs private and public interests that militate against disclosure. In all of these situations, there should be legal constraints on use by the recipient and prohibitions on redisclosure.

## *ENDNOTES*

1. This discussion borrows from Dr. Ruth Faden, ***Conceptual Issues in Maintaining the Balance Between the Privacy of Private Sector Health Records and the Need for Information,*** Presented at the DHHS Conference on Health Records: Social Needs and Personal Privacy. Washington, DC. February 11, 1993.

2. It is not clear how great this "chilling effect" would be. Some authorities have doubted that there would be any substantial effect, and have accordingly questioned whether there should be any privilege for such communications. See 8 John Wigmore, ***Evidence*** §§ 2380a, ***2285*** (John McNaughton rev. ed. 1961). However, it appears that many individuals are altering their relations with the health care system precisely in order to keep certain kinds of health information away from persons who would otherwise obtain it. The Privacy Protection Study Commission found that the prospect of records disclosure does deter individuals from seeking treatment, at least with respect to psychological conditions. Privacy Protection Study Commission, ***Personal Privacy in an Information Society.*** Washington, DC: Author. 1977:286. The Advisory Committee on the Federal Rules of Evidence would have codified into federal law a limited privilege, applying only to psychotherapist-patient communications; its recommendations were not ultimately adopted. See 56 F.R..D. 183, 240-42 (1973) (proposed Fed. R. Evid. 504). People taking genetic tests often pay large sums of money out of pocket in order to keep the information away from insurance companies, out of fear that disclosure to the insurance companies would render them uninsurable. See Statement of Nancy S. Wexler, Ph. D., Chairperson, NIH/DOE Working Group on the Ethical, Legal, and Social Issues of the Human Genome Project, lbefore the House Committee on Government Operations Subcommittee on Government Information. October 17, 1991: 12. The Privacy Protection Study Commission recounted an incident where the prospect of disclosure of detailed psychological information to insurance companies had deterred individuals from filing insurance claims for those services. Privacy Protection Study Commission. 1977:286.

3. Privacy Protection Study Commission. 1977:306.

*4.* Privacy Protection Study Commission. 1977:313.

*5.* At that time the Privacy Protection Study Commission supported a Federal role in protecting medical-care records that built "on existing regulatory mechanisms and current certification and accreditation processes. " Privacy Protection Study Commission. 1977:293. It also recommended federal statutory protection against government access to personal records, including medical records. Privacy Protection Study Commission. 1977:294, 362-89. However, it left the basic protection to the States. Privacy Protection Study Commission, 1977:292-95. The division of responsibility between the Federal Government and the States proposed by the Commission was partially based on some hesitation about

imposing the rules by law or regulation on individual health care providers at the time the recommendations were made. Institutions were subject to accreditation and certification processes to qualify for Medicaid and Medicare participation, individual practitioners were not. The Commission's more general theory of the Federal and State roles in privacy protection was based on recognizing and encouraging the existing role of States; the specifics of protection would take various forms, depending on whether the subject area was traditionally a matter of State regulation. Privacy Protection Study Commission. 1977:494.

6. Faden. 1993.

7. Faden R, Beauchamp T. ***A History and Theory of Informed Consent. New*** York, NY: Oxford University Press. 1986.

***8.*** Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R, Steinauer D. ***Privacy and Security of Health Care Information.*** Prepared for the President's Health Care Reform Task Force. Washington, DC. June 2, 1993.

9. Flaherty DH. ***Ensuring Privacy and Data Protection in Health and Medical Care.*** Presentation at Kennedy Center of Ethics, Georgetown University, Washington, DC. April 5, 1993.

10. Beauchamp TL, Childress JF. ***Principles of Biomedical Ethics, 3rd Ed. New*** York, NY: Oxford University Press. 1989: 107.

11. Beauchamp. 1989: 108-109.

12. Privacy Protection Study Commission. 1977:314.

13. Statistics Canada. ***Informed Consent Form: The Self-Sufficiency Project.*** Ottawa, Canada: Author. 1992: 11-19.

14. American Medical Record Association. ***Confidentiality of Patient Health Information.*** Chicago, IL: Author. 1985.

15. Privacy Protection Study Commission. 1977: 3 15.

16. Privacy Protection Study Commission. 1977:315.

17. This basic categorization is suggested in a study by the Intergovernmental Health Policy Project of George Washington University. See Intergovernmental Health Policy Project. ***Laws Governing Confidentiality of HIV-Related Information, 1983-1987.*** Washington, DC: George Washington University. 1989:I-19.

18. Intergovernmental Health Policy Project. 1989: I-6.

19. American Hospital Association. ***Guidelines: Institutional Policies for Disclosure of Medical Record Information.*** Chicago, IL: Author. 1979:3.

20. Privacy Protection Study Commission. 1977:306,308.

21. Cal. Health & Safety Code § 199.25 (West 1988).

22. Id. § 1797.188 (West 1988); Cal. Penal Code §§ 1524.1, 7522 (West 1988). The 1989 study found that 20 states had laws allowing unconsented disclosure to individuals who had sustained a significant exposure to HIV. Intergovernmental Health Policy Project. 1989:I-6.

Even this situation raises difficult issues. Some states allow informing health care workers that a patient is HIV-positive before treatment. See, e.g., N.J. Stat. Arm. § 26:5C-8(b)(3) (West Supp. 1990). The justification for such disclosure weakens if health care workers follow the recommendations of the Centers for Disease Control to take precautions against HIV transmission in all situations because they can never be certain which patients are infected. See CDC, Recommendations for Prevention of HIV Transmission in Health-Care Settings. ***Morbidity & Mortality Wkly. Rep.,*** Supp. No. 2. 1987:32. However, it has been argued that workers cannot maintain such uniform vigilance, and that they would exercise extra caution if they knew that a particular patient was HIV positive. Jeff Glenney, Note, ***AIDS: A Crisis in Confidentiality, 62 S.*** Cal. L. Rev. 1701, 1718-20 (1989).

23. 1988 N.Y. Laws 9265-A, § 2782(l)(d).

***24*** Wexler NS. 1991.

***25*** Steven Findlay, If Your Doctor Has AIDS, U.S. News & World Rep., Feb. 18, 1991, at ***66***

***26.*** Eileen Hansen & Tom Steel, HIV Testing: Policies, Policy and People, The Recorder, Sept. 13, 1991, at 5.

***27.*** See Estate of Behringer v. Medical Center, 592 A.2d 1251 (N.J. Super. Ct. 1991).

***28. See*** generally Agency for Health Care Policy and Research. Grady ML, Schwartz HA, eds. ***Medical Effectiveness Research Data Methods.*** Washington, DC: Author. 1992.

29. If health information is transferred without identifiers, in circumstances that make it very unlikely that the recipient will try to identify the individuals, and where the information will be used in a way that does not directly affect the individuals, this probably should even not be treated as a disclosure. John Fanning has suggested such a distinction. See John P. Farming, ***HIV Infection and the Future of Confidentiality Policy.*** Remarks presented at the Public Health Conference on Records and Statistics. Washington, DC. July 18, 1989:6. To treat such a communication of information about unidentified individuals as a disclosure risks

creating confusion about other communications that do not identify individuals. The federal Privacy Act has caused this kind of ambiguity by listing this kind of communication among the permitted disclosures of records. 5 U.S.C. § 552a(b)(5), (a)(6). It is appropriate for a statute to address this issue and to define when such communications will be allowed, but it should do so separately from the provisions listing permitted disclosures without consent.

30. These determinations are substantially modeled on the standards recommended in the Privacy Protection Study Commission. 1977:306.

3 1. The Department of Health and Human Services has advocated a very similar set of restrictions. Hunter ND. *Testimony before the Subcommittee on Information, Justice, Transportation, and Agriculture, Committee on Government Operations, U.S. House of Representatives.* Washington, DC. April 20, 1994.

32. Intergovernmental Health Policy Project. 1989:I-19 to I-20.

33. Fanning. 1989:8.

34. Intergovernmental Health Policy Project. 1989: I-2 1.

35. These conditions are modeled on the Privacy Commission's recommendations. See Privacy Protection Study Commission. 1977:307, 310.

36. "Discovery" includes depositions, interrogatories, and requests for production of documents in litigation. See Fed. R. Civ. P. 26-37. The Privacy Commission limited its discussion to attempts by the Government to obtain records themselves. See Privacy Protection Study Commission Report. 1977:362-63,365. However, the same issues arise with attempts by private litigants to use judicial process (or the process of an administrative tribunal), and with attempts to obtain health information about identified individuals by questioning the health care provider or record keeper, even without physical disclosure of the records. The discussion here thus covers all such methods of obtaining health information.

37. The Privacy Commission described these problems well. See Privacy Protection Study Commission. 1977:351-52. Even the exception in the Privacy Act of 1974 for disclosures from a federal agency's system of records to a law enforcement agency is too permissive. It allows an agency to disclose records based only on a written request from a supervisor in the law enforcement agency, stating which portion of the record it seeks and the law enforcement activity for which the record is sought. 5 U.S.C. § 552a(b)(7); Office of Management and Budget, Guidelines on Privacy Act Implementation, 40 Fed. Reg. 28947, 28955 (1975). It requires no notice to the individual, no balancing of interests, no finding by a neutral arbiter, and no restrictions on use or redisclosure by the recipient. The Social Security Administration has tried to impose some restrictions on its own discretion to supply records to law enforcement agencies by limiting such disclosures to situations involving serious crimes or crimes relating to the Social Security program. See 20 C.F.R. § 401.315 (1993).

***38. See, e.g.,*** Ill. Admin. Code tit. 77, § 693.000 (1988); 1988 N.Y. Laws 9265-A, § 2785. The Privacy Act provision for unconsented disclosure based on a court order fails to impose any such substantive limitations. See 5 U.S.C. § 552a(b)(11). It thus allows an agency to disclose records in a litigation context by merely signing a stipulation with the other party and submitting it to the judge for his or her signature, which transforms it into a court order.

39. The Privacy Act provision allowing unconsented disclosure based on a court order is construed this way, as not allowing disclosure in response to a grand jury subpoena. Doe v. DiGenova, 779 F.2d 74, 85 (D.C. Cir. 1985) (construing 5 U.S.C. § 552a(b)(11)).

40. The Privacy Protection Study Commission recommended giving the individual notice and an opportunity to appear and oppose disclosure only where he or she was a party to the underlying litigation, was a likely target of the investigation, or would otherwise be publicly implicated in the proceedings (presumably in a way that would identify the individual or would make him or her reasonably identifiable). Privacy Protection Study Commission Report, 1977:373, 379. (The Commission's recommendations with respect to administrative subpoenas included a similar but slightly broader exception. ***Ibid. 371.)*** Some such limitation is reasonable -- if an investigation or action focuses on the recordkeeper's conduct, there may be a need for access to hundreds of individual records, so affording notice and an opportunity to appear could create immense procedural burdens. At the same time, since the action focuses on the recordkeeper, there will be less danger that disclosure will harm the individual substantially. Still, disclosure without notice and opportunity to appear should be limited to situations with large numbers of records, and the statute should impose strict limits on use and dissemination of that information in reasonably identifiable form.

## *INTRODUCTION*

This section examines the impact of automation on the privacy of health information. The development of security standards and the protection of computerized systems are also addressed.

## *BACKGROUND*

### Automation of Patient Records

Although health related records have long existed in automated form, they have tended to support specific functions such as the laboratory, pharmacy, or financial department of a health care institution. A dramatic shift in how health related information is collected and stored is now underway. Patient specific, computer based records containing the full spectrum of medically related data collected over a person's life span are being developed. Renewed impetus for development of these computer based systems was provided by the Institute of Medicine's report, The ***Computer-based Patient Record: An Essential Technology for Health Care,*** published in 1991, which recommended that computer based patient records be developed to improve patient care and the management of health care data.' The Computer-based Patient Record Institute, established in 1992, was a direct outgrowth of recommendations in this report.

While particular groups may visualize these computer based patient records somewhat differently, those focusing on development of automated health care systems, such as the Computer-based Patient Record Institute, the Medical Record Institute, and the American National Standards Institute, see a system of several parts emerging in the next decade:[2]

- **a comprehensive, longitudinal, computer based patient record -** containing all clinical, financial, and research data, including diagnostic images and pictures .[3]

- **a "national" electronic network** for accessing the health records for a variety of purposes such as primary care, insurance payment, peer review, cost containment, public health, and research purposes.[4]

- **a smart card component** for an array of purposes such as providing health insurance coverage information, documenting services, and providing a conception-to-death record of all health care.

- **use of unique patient-specific identifiers** within a country and perhaps, world wide.

The health care industry believes the technology for implementation of paperless computer based record systems is becoming available.[5] The Institute of Medicine (IOM) report stated:

> Most of the technological barriers that formerly impeded development of CPR (..computer based record. .) systems have either disappeared already or are about to dissolve. Nevertheless, although no technological breakthroughs are needed to realize CPR systems, further maturation of a few emerging technologies, such as hand-held computers, voice-input or voice-recognition systems, and text-processing systems may be necessary to develop state of the art CPR systems in the 1990s. In some cases, promising technologies must be tested further in "real life" situations; in other cases, technologies that have proved beneficial in applications in other fields must be adopted for use in health care. [6]

Related efforts supporting the development of automated health information systems are underway. Under the Bush Administration, the Federal government and the health insurance industry began working on an insurance identification and eligibility system that will include electronic claims transfer and an automatic payment system. With strong leadership from Vice President Gore, the Advisory Council on the National Information Infrastructure was formed to advise the Secretary of Commerce on development of the national information infrastructure consisting of "integrated hardware, software and skills that make it easy and affordable to connect people with each other, with computers, and with a vast array of services and information resources. "[7] A Federal agency-wide Information Infrastructure Task Force established by the Department of Commerce is focusing on development of a prototype national network for the electronic interchange of library, educational, governmental, and health information.

Integral to these efforts is the development of standards for the contents of patient records and for communications protocols which permit data to flow across discrete systems to the diverse groups who must legitimately access health information. Security standards must also be developed. According to the IOM report:

> In addition to further development of necessary technologies, a variety of standards must be developed, tested, and implemented before the CPR can realize its full potential at both the macro (e.g., epidemiological) and micro (e.g., physician office) levels. Standards to facilitate the exchange of health care data are needed so that clinical data may be transmitted on networks or aggregated and analyzed to support improved decision making. Standards are also needed for the development of more secure CPR systems.. .[8]

Security standards, however, can be no more effective in protecting personal health information than existing legislation and other directives governing access.

Automated systems now under development or coming online are increasing the amount of health data stored in an electronic format and improving the ease with which these data can be accessed. Software systems are now available that facilitate the rapid extraction of data from a variety of sources and the reintegration of these data into new sources of information.

Software tools such as graphical user interfaces (GUIs), relational data base systems (RDBMSs), and computer assisted systems engineering (CASE) tools are making it easier for technical and non-technical persons to develop electronic medical records systems.' Data standards and the availability of data dictionary systems are making access to the data easier for these persons. Finally, open systems architecture is facilitating communications among disparate local area networks (LANs) and systems. A Washington Post article about Internet quoted Jeff Ashurst, a resident of Britain, responding by E-mail to a Washingtonian's electronic query, "The size of the planet is no boundary to communications".[10]

**Card Technology**

Technology is also emerging which may allow plastic wallet-sized cards to store significant amounts of information and to interface with computing systems. This new card technology includes embossed cards, magnetic stripe cards, integrated circuit cards (i.e. memory chip cards and smart cards), and optical storage cards. Each type of card varies in the amount of information that can be stored on it and the level of security that it can provide. Embossed cards contain only the information appearing in raised letters on their surface. Magnetic stripe cards utilize one or more magnetic stripes to record information. They tend to be used to access central data bases and processing facilities through communications networks. Integrated circuit cards utilize microchips embedded in their surfaces. Memory chip cards can only be used to store information while other "smart" cards may permit the manipulation of stored information. Optical storage cards can be written on only once. Information can be added to but not deleted from optical storage cards. Additionally, they are durable and can be read many times.

Within the health care sector, and depending upon the technology selected, these cards could serve a variety of purposes ranging from health insurance identification to the storage of complete medical records.[11] To date, these cards have been primarily used in Europe for a variety of applications ranging from banking and financial transactions to medical applications.[12] In Canada, there is a trend toward using magnetic stripe cards as personal health cards. The Working Group on Electronic Data Interchange contends that other countries are selecting smart cards as an alternative to accessing central computer systems because their communication systems lack the sophistication and reliability of the networks available in the U.S. They further point out that implementing this technology in the United States could cost hundreds of millions of dollars given equipment costs, installation, and training required to support the technology.[13]

**Implications of Automation for Privacy Protection**

As Alan Westin pointed out as far back as 1969: "... we are building hundreds of data bases with communications networks uniting them; they are outgrowths of the ways in which we have always kept records, files, dossiers, and information; but in terms of the quantity of the information, its sensitiveness, and the speed with which it circulates, through the evaluative system of the society today, these systems present a problem of new dimensions".[14] Indeed, the development of electronic health care networks permitting standardized patient based information to flow nationwide, and perhaps even worldwide, will require dramatic shifts, both in how privacy and confidentiality are viewed, and in how legislation protecting individual privacy is crafted. Collin J. Bennett has argued that "...legislation such as the U.S. Privacy Act (1974), the Canadian Privacy Act (1982), and the British Data Protection Act (1984) were designed to solve the problems inherent in a generation of information technology that has already been surpassed. The *first generation* of data protection statutes has already been rendered obsolete by new forms of information control and surveillance techniques."[15]

These issues are not only relevant to the United States, but internationally as well. Collin Bennett, comparing privacy protection laws in the United States, Canada, Britain, West Germany and Sweden, stated:

> Most data protection laws are based on some notion of identifiable "system of records" that can be counted and published for the benefit of those who might want to access individual records. There is persuasive evidence, however, that the definition of personal information systems is now arbitrary and somewhat meaningless. The direct linkage of computer records via telecommunications systems allows for easier disclosure and exchange of information than was previously the case. Online access via telephone lines or local networks gives bureaucracy the capacity to assemble information selectively and to correlate and analyze information in different ways from those envisaged when it 'was first collected. This is functionally equivalent to the creation of new data.
>
> Another critical factor in the 1980s has been the microcomputer, which decentralizes the power of information collection, storage, and retrieval, and the exchange in the hands of discrete individuals. In the early 1980's, when computers first made their appearance in organizations, they were expensive, cumbersome, and required considerable skill to operate.. . .Now , the astounding progress made in microelectronics has rendered the computer more manageable, less expensive, and more "user friendly." The proliferation of computers complicates the process of protecting personal information: individual users can effectively create their own systems of records and can use microcomputers as remote terminals to access larger systems" In the United States, the networking of the [F]ederal government is, according to the Congressional Office of Technology Assessment (OTA), "leading rapidly to

> the creation of a de *facto* national database containing personal information on most Americans". ....[16]

He points out that networking has facilitated at least three new surveillance practices: computer matching or record linkage, computer assisted front end verification to certify claims, and computer profiling to identify classes of persons likely to engage in particular kinds of behavior."

The development of new protections must begin with consideration of what information about individuals should be collected and with whom this information should be shared. These decisions require judgements about the tradeoffs between "rights to privacy" and the value of information to both the individual and to society. Given this broader framework, the current focus on systems of relatively fixed records will need to be radically altered. It must reflect the growing ease with which individual units of information can now be combined and recombined both within and across organizations thereby creating multiple "record systems". Access rules will continue serving as one of the major mechanisms for regulating the flow of computerized information. However, protecting privacy will require attaching privacy protections to the individual units of health information themselves, rather than to the original "record system" which generated the information.

Moreover current requirements that make the institution developing a record responsible for protecting it are no longer adequate. As John Fanning has stated:

> Our past thinking basically assumed a paper record, that existed in one place, and which could be duplicated only by a rather deliberate effort. We may also have had in mind a computer system in which everyone who could call up the material was part of the institution which created the record, or was part of another institution which has an explicit agreement -- written, in advance -- with the one that created the record, prior to the point at which the record was being called up on the screen.. . If we permit disclosure to people outside the health care system subject to certain restrictions (e.g. disclosure pursuant to a court order) who can disclose? Is it just the organization where the record was made? Or is it anyone in the health care system who can call it up on the screen? [18]

Use of card technologies raises additional privacy concerns. They have been carefully described by the Privacy Commissioner of Ontario: [19]

- Ownership - of the information contained in the card must be determined since the owner is responsible for ensuring privacy protections.

- Access - with the information readily available in machine readable form, it may be difficult to prevent those health care providers with

access to the card from copying information into their own files. This could result in the proliferation of unintended databases containing health information.

Furthermore, the increased availability of health information through the use of cards increases the risk of unauthorized and/or inappropriate collection, retention, use and disclosure of this information. The question of how decisions regarding access to the card will be made, and who will be responsible for monitoring access to personal information, must be addressed. It is also necessary to determine how the individual's right to access and correct information on the card will be ensured.

**Standards Development Efforts**

The need for protection of computer based patient record systems is widely acknowledged by those working on the development of electronic health care systems. At least fifteen different, primarily nongovernmental, confidentiality committees are now working on standards development. There seems, however, to be a wide gap in the approach and scope of differing groups' efforts due to a lack of consensus on appropriate confidentiality measures and national goals.[20] Many of these groups agree that the Federal government should play a leadership role in coordinating efforts to develop standards, including those related to privacy policy. While they question whether existing voluntary efforts are adequate, there is also strong feeling that voluntary efforts should continue to be a major source of future developments. A just released GAO report,[21] recommends that the Federal government assume a general leadership role with respect to standards development.

Currently, the majority of standards in the U.S. are developed through a voluntary consensus process with participation from both the public and private sectors. Within the Federal government, the Omnibus Budget Reconciliation Act of 1989 assigned responsibility to the Agency for Health Care Policy and Research (AHCPR) within the Department of Health and Human Services for developing automated medical record standards. AHCPR has pursued this objective by actively supporting the American National Standard Institute's Health Informatics Standards Planning Panel which is coordinating the various voluntary standards activities in the United States and serving as a liaison for European standards work. Other Federal agencies' involvement in medical records standards development has primarily been through participation in voluntary organization meetings. These agencies include the Health Care Financing Administration, the Department of Defense, the Department of Veterans Affairs, the National Highway Traffic Safety Administration and the Consumer Product Safety Commission. More broadly, the Department of Defense has accounted for most Federally developed standards. The Department of Commerce, through its National Institute of Standards and Technology, has also assisted both the public and private sector in developing standards. [22]

Department of Health and Human Services (DHHS) Secretary Donna Shalala, in testifying before the House Appropriations Subcommittee in February of 1993, stated that DHHS was requesting $9 million for the National Library of Medicine to develop technologies for high

performance computing and high speed networking in the health care sector. She further stated that "...in the future, modem information technologies have the potential to improve health care dramatically, while at the same time reducing its costs." She noted that funding will also improve progress toward the creation of national standards for electronic records which are necessary to ensure patient privacy as well as to eliminate redundant testing and lost patient charts. [23]

*CONFIDENTIALITY AND SECURITY OF AUTOMATED SYSTEMS*

The National Research Council, System Security Committee, in it's recent report, *Computers at Risk: Safe Computing in the Information Age* states that, "the nation needs computer technology that supports substantially increased safety, reliability, and, in particular, security. "[24] They further defined security as:

> ...protection against unwanted disclosure, modification or destruction of data in a system, and also . . the safeguarding of systems themselves. Security, safety, and reliability together are elements of system trustworthiness--which inspires the confidence that a system will do what it is expected to do.[25]

As automated health care records systems are developed and utilized to transmit standard health care information nationwide and perhaps worldwide, over electronic networks, "society becomes more vulnerable to poor systems design, accidents that disable systems, and attacks on computer systems". [26] Opportunities for using electronic health care networks may be lost if there is serious mistrust of their safety. Security standards can be used to strengthen patient privacy and confidentiality and assure that information is available to improve the quality and efficiency of health care services. As stated by Alan Westin in 1969:

> Here is the dilemma. The computer is threatening our levels of privacy as never before, but it also offers more protection of privacy than we have had heretofore. As always, the machines are neutral. The answer depends on what man will do with them.[27]

With existing paper systems, requests for information often result in the release of data that are not pertinent to the current request because whole documents are copied and transmitted to requestors. In contrast, computerized systems facilitate the selection and retrieval of identified data items from an individual health record, making it possible to share only the information that is necessary to a specific inquiry. Establishing appropriate access requirements for computer systems can result in more accurate, reliable, and cost efficient protection of health care information than is presently available with paper records. It is also possible to maintain detailed records (audit trails) of access to information. Audit trails are not as practical with paper systems. Even with automated systems, they tend to be less effective when there is repeated redisclosure of information.

Recent advances in computer technology facilitate access to data in ways that were not possible with paper systems and increases the potential for secondary uses of data. A single breach of security can result in retrieval of a large amount of information about numerous individuals and indiscriminate distribution of this information. Computerization will soon allow facile linking of data sets and may increase the potential for unauthorized release of information and, consequently greater intrusiveness into individuals' records and lives. Further, records can easily be transmitted across State lines, making it difficult for any State to offer reasonable protections. Individuals find it difficult to understand where information about them resides, how it is used, and how information is linked. Easy movement of records also makes it difficult for individuals to effectively control the redisclosure of information.[28] Computerization increases the amount of available information about an individual. As stated by Gary T. Marx:

> With massive computerized "jackets" on everyone so easily accessible, the past is likely to become increasingly important in structuring individual opportunities. Persons may never cease paying for earlier misdeeds. Aside from the possibility of locking in erroneous or sabotaged data, this may have the unintended consequence of permanent stigmatization. It may even increase commitment to rule breaking. Those who wish to lead law abiding lives may face increased difficulties as a result of electronic branding. Starting over may prove to be more than difficult.[29]

He further notes that individuals may decline needed services, such as mental health treatment, for fear of what might appear in their record.

**Computer Security Technology**

Although ensuring total security of a computer system will never be feasible, there is much that can be done to protect records.[30] With cognizance of the issues, careful planning, and timely action, it is possible to not only address current privacy and security concerns for health care information, but to actually *improve* the degree of protection. To be effective in the rapidly changing health data automation environment, data protection policies must establish privacy protection guidelines and standards that define system goals. In contrast, tying policies and standards to specific systems and system capabilities could result in their becoming obsolete before they are fully implemented. Privacy protection will be most effective if the issue is addressed directly at the initiation of computer based patient record system development. The policies should guarantee that only those with authorized access are able to access records for authorized purposes at authorized times.

The adequacy of data security systems can also be evaluated against known threats to confidentiality. Threats to confidentiality can emerge from outside an organization, as well as among an institution's own personnel. The security system should be designed to address any perceived type of threat. Regular security checks should be conducted and recorded.

Effective security protection for health care information will require use of technology that is not typically used in most computer systems and networks today. While the technology exists and has been shown to be effective and affordable, it is not widely used because it must either be retrofitted to existing systems or because it is perceived to be costly or inconvenient.

An important privacy and security issue is the valid concern by health professionals that computer security may slow down the flow of required information needed to provide adequate and timely health care, especially in an emergency situation. Those working on the development of security systems for computerized health care applications are addressing these concerns .[31]

The steps identified by the National Research Council as necessary for achieving greater computer security and trustworthiness are as applicable to health computer systems as to those systems serving other purposes. These steps include promulgating a comprehensive set of "Generally Accepted System Security Principles" which would provide a clear statement of essential security features, assurances and practices.[32] Among the major elements of these principles are quality control, access control on code as well as data, user identification and authentication, protection of executable code, security logging, a security administrator, data encryption, operational support tools to assist in verifying the security state of the system, independent audits of the system and hazard analysis. Levels of access can also be established recognizing the varying degrees of security required for different types of information.

Because computer technology is rapidly evolving, it will be necessary to conduct the research needed to ensure that technical advances do not erode security practices. Oversight and management structures are also needed to promote the development and proper use of system security principles in the development and implementation of health care data systems.

**Institutional and Professional Responsibilities**

In addition to establishing policies that place requirements on patient record systems, and networks in which these records are stored and transmitted, it is also important that confidentiality policies be established for individuals and organizations who gain legitimate access to patient records through networking, computer sharing, and/or outside computer services contracts. Most breeches of security that now occur are the result of "insider" action. Routine institutional review and monitoring can be used to evaluate the appropriateness of access and security measures. Training programs should be instituted so that employees are fully aware of their responsibilities and the actions required of them in performing their jobs. These issues are discussed fully elsewhere in this report.

*SUMMARY*

It is anticipated that the physician held paper medical record will evolve into a longitudinal, comprehensive computer based patient specific record containing a wide variety of health

related information that will be accessible as a part of a national health data network. These changes are accompanied by recent technological innovations that include the availability of software tools that increase access to computer stored data by nontechnical persons and facilitate the integration of data from a myriad of sources into new systems of records; open architecture that facilitates data flow across systems, institutions, States, and nations; and smart cards that could allow health related information to become portable. These changes will impact on the privacy of health information, including access and ownership of data.

The conceptual and technical changes to health related information can increase the risk of unauthorized and/or inappropriate collection, retention, use and disclosure of this information. On the other hand, automation may afford greater privacy protections as audit trails monitor access to the data. In addition, only the relevant parts of a medical record need to be transmitted to respond to requests for reimbursement, documentation, or other activities. The development of electronic health care networks that permit standardized patient based information to flow across institutions and geographic regions will require major changes in how privacy and confidentiality are conceptualized and how legislation protecting individual privacy is crafted. The current State level privacy protections are no longer adequate. Records can be made instantaneously available over Electronic Super Highways, rendering location an obsolete concept.

Security standards needed to govern access to health care systems, are being developed in both the private and public sectors and will evolve as automation continues. Issues of access to health related information, assignment of responsibility for monitoring access to personal information, and individuals' rights to access and ensure the accuracy of information must all be addressed.

## *ENDNOTES*

1. Dick RS, Steen EB, eds. *The Computer-based Patient Record: An Essential Technology for Health Care.* Washington, DC: National Academy Press. 1991.

2. This definition is derived from the definition used by the Computer-based Patient Record Institute, Chicago, Illinois.

3. Dick RS, 1991. "Medical imaging today includes diagnostic images or pictures obtained from film scanners, computed radiography (CR), magnetic resonance (MR), computed tomography (CT), ultrasound and nuclear medicine sources." While these images are typically two-dimensional still pictures, the increasing digitization of data is rapidly expanding horizons for computerizing data providing significantly additional informational value.

4. Dick. 1991:65. The editors point out that the advent of fiber optics is permitting transmission of a diversity of information at high speeds and low costs. Also see, The *Report of the Workgroup for Electronic Data Interchange to the Secretary of U.S. Department of Health and Human Services,* July 1992 (co-chaired by Joseph T. Brophy and Bernard R. Tresnowski) which states on page 2: ". ..The desired result is a health care industry, connected by an integrated system of electronic communication networks which allows entities within the health care system to exchange information and process transactions, with appropriate safeguards to ensure that privacy and security interests are protected. ED1 (electronic data interchange) technology is already available although being used on a limited scale and without uniform procedures. It is anticipated that communication networks will evolve through interconnections among various existing and new networks, rather than by creation of a single national architecture.. .."

5. The discussion in the paragraph is a synopsis of information contained in *Toward an Electronic Patient Record: Update on Standards and Developments.* Newton, MA: Medical Records Institute. June 1992;I(1).

6. Dick and Steen. 1991:2.

7. Statement of the White House Office of the Press Secretary, President William J. Clinton, in an Executive Order, United States Advisory Council on the National Information Infrastructure. September 15, 1993.

8. Statement of the White House Press Secretary. 1993.

9. Graphical user interfaces, such as Windows, allow users to choose options by pointing to a graphic icon and activating the choice with either a keyboard or a mouse. The icons only have to be learned once and then can be applied to multiple software programs. A relational database system is designed to take advantage of relationships among various groups of data.

Once developed it can be used by many persons without the need for extensive knowledge of the processes used to establish the relationships. CASE tools permit users to create computer code without knowing programming languages.

10. Burgess J. Internet creates a computer culture of remote intimacy. The ***Washington Post.*** Monday, June 28, 1993:A1-8.

11. Wright T., Commissioner. ***Health Card Technology: A Privacy Perspective, Information and Privacy Commissioner.*** Ontario, Canada. October 1992:3-4.

12. Dick. 1991;footnote 16:78.

13. The Work Group on Electronic Data Interchange. 1992:34.

14. Westin A. Computers and the protection of privacy. ***Technology Review.*** April 1969;71(6):36.

15. Bennett CJ. Computers, personal data and theories of technology: Comparative approaches to privacy protection in the 1990s. ***Science, Technology, and Human Values.*** Sage Publications. 1991;16(1):53.

16. Bennett. 1991:53-54. The citation is taken from the U.S. Congress, Office of Technology Assessment. ***Federal Government Information Technology: Electronic Record Systems and Individual Privacy.*** Washington, DC: Government Printing Office. 1986: 102.

17. Bennett. 1991:54.

18. John Fanning addressed this issue in his April 1, 1993 memorandum, ***Musing of John Fanning on Legal Controls for Information Held in Computerized Systems.***

19. Wright. 1992:i-ii.

***20.*** Information in this paragraph is paraphrased from ***Toward an Electronic Patient Record: Updates on Standards and Developments.*** Newton, MA: Medical Records Institute. January 1993;I(6).

21. General Accounting Office, Information Management and Technology Division. ***Automated Medical Records: Leadership Needed to Expedite Standards Development.*** Washington, DC: US Government Printing Office. 1993. GAO/IMTEC-93-17.

***22.*** U.S. General Accounting Office. ***ADP Systems: Automated Medical Records Hold Promise to Improve Patient Care, Report to the Chairman.*** Washington, DC: Senate Committee on Government Affairs. 1991. U.S. GAO Publication, GAO/IMTEC-91-5.

23. Shalala DE. ***Testimony of the Secretary of Health and Human Services before the U.S. Congress, House Appropriations Subcommittee on Labor, Health and Human Services and Education.*** Washington, DC. 1993.

24. National Research Council, Systems Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications. ***Computers at Risk: Safe computing in the information age.*** Washington, DC: Author. 1990.

***25.*** National Research Council. 1990.

***26.*** National Research Council. 1990: 1.

***27.*** Westin. 1977:33.

***28.*** These issues have been covered in many of the already cited references as well as other sources including Rothfeder J. ***Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret. New*** York, NY: Simon & Schuster. 1992; ***Toward an Electronic Patient Record: Updates on Standards and Developments. Newton,*** MA: Medical Records Institute. January 1993;I(6); Department of Health, Education and Welfare. ***Records, Computers and the Rights of Citizens.*** Washington, DC: Author. 1973; and Waller AA. Legal aspects of computer-based patient records and record systems. In: Dick RS, Steen EB, eds. ***The Computer-Based Patient Record, Institute of Medicine.*** Washington, DC: National Academy Press. 1991; 157-177.

Similar concerns have been expressed by Computer Professionals for Social Responsibility (CPSR) regarding computerization more generally. In his testimony before the Subcommittee on Government Information, Justice and Agriculture, Committee on Government Operations, U.S. House of Representatives, May 16, 1990, Mark Rotenberg who directs CPSR's Washington Office stated "there is little question that new computer technology has made it easier for large organizations to collect and exchange data. And it has made possible inferences about individual behavior based on this information. Computer technology has spawned an enormous proliferation of detailed transactional data that can be used for purposes detrimental to the interests of the person involved. The problem today is that there is inadequate policy guidance to ensure the protection of privacy for this personal information. "

***29.*** Marx GT. The iron fist and the velvet glove: totalitarian potentials within democratic structures. In Short JE, ed. The ***Social Fabric: Dimensions and Issues.*** Beverly Hills, CA: Sage Publications. 1986.

***30.*** Rotenberg M. ***Privacy in the Computer Age.*** Palo Alto, CA: Computer Professionals for Social Responsibility. 1989.

***3*** 1. This issue was discussed in many sessions of the American Medical Informatics Association's Sixteenth Annual, ***Symposium on Computer Applications in Medical Care,*** held on November 8 through 11, 1992 in Baltimore, MD.

32. National Research Council. 1990. This section draws heavily on discussions contained on pages 4 through 6 and pages 28 and 29.

## *A UNIQUE PERSONAL IDENTIFIER*

### *INTRODUCTION*

This section examines why a unique personal identifier for health records is needed, reviews suggested options and addresses some of the broader issues regarding the use of identifiers. Although a name may be considered a personal identifier, more than one person can have the same name. A *unique personal identifier* is a number or other identifying code that identifies one, and only one, individual.

### *BACKGROUND*

The Privacy Protection Study Commission (PPSC) pointed out that "in a modern society labels have become essential for identifying an individual and selecting information about them from a set of records and for authenticating that a record does indeed belong to a particular individual. "[1] They further state:

> As long as individuals have established relationships with organizations, personal identification and authentication have been important processes. For organizations which maintain records in order to facilitate their relationships with individuals, a record identification and authentication procedure within the organization is essential. As organizations, and the populations served by them increase in size, the importance of identifying and authenticating the records which document and mediate interactions between organizations and individuals grows correspondingly. And, whenever organizations exchange records about an individual, inter-organizational identification and authentication is crucial. In such cases the identifiers and authenticators used by the organizations between which exchanges of records take place must be common to both. This is one important reason why the use of a few widely available labels, such as the SSN . .(Social Security Number).., has become pervasive. [2]

The Commission reported that opposition to the use of labels stems, in part, from a few individuals resenting being identified by a number, or other identifying code, rather than by name, which they view as dehumanizing. For them, no matter what label is used, it would arouse opposition. Others are concerned about the use of particular labels, most notably the SSN.[3] The Commission also pointed out the benefits to individuals that derive from record systems using labels for identification and authentication purposes:

> As long as organizations have relationships with individuals, most of whom are not known personally by someone within the organization, effective personal identification and authentication is an essential social mechanism. As long as organizations make decisions about individuals on the basis of recorded information, some means of assuring that the information being used does

> indeed pertain to the individual affected by the decision is necessary. It should also be clear that while accurate identification and authentication facilitates the work of organizations, it also benefits individuals who seek fair and prompt decisions from them. If individuals and records are not correctly identified and authenticated, an individual may be unfairly denied a right, benefit, or opportunity as a result. Society as a whole also suffers when a benefit is given to an undeserving individual. In sum, accurate identification and authentication are an essential component of fairness in record keeping.[4]

There is a growing need for the use of some form of unique label (e.g. identifier) for identifying health related information pertaining to a particular individual. Indeed, efforts to develop longitudinal computer based health records about individuals which are available over electronic networks are already underway.' The Clinton Administration has also shown strong support for the development of automated health information systems both as part of its health care reform proposal and in its plan for investing in technology. The Administration has specifically mentioned the need to improve access to information in health care as one of the driving forces behind development of a national information infrastructure and "information superhighway. "[6] The Agenda for Action of the National Health Information Infrastructure Task Force states that "telecommunications applications could reduce health care costs by $36 to $100 billion each year while improving quality and increasing access.'

In general, the systemic changes which have been put forward in the past few years for administrative simplification and/or reform of the health care system tend to require significant additional development of automated systems providing standard longitudinal information on individuals.[8] These automated systems will require use of a unique identifier for collecting, managing and utilizing information about an individual.

## *OPTIONS FOR A UNIQUE PERSONAL IDENTIFIER*

Although clearly needed, use of a unique personal identifier raises significant privacy concerns. Perhaps the most critical single decision regarding privacy and security in a highly automated world is what this unique identifier should be and what types of record linkages should be permitted. There are two main alternatives: using the Social Security Number or creating an entirely new numbering system. The advantages and disadvantages of these options are discussed below. Ultimately, it may matter little what alternative is chosen. That is, without clearly established rules for permitted uses of the information that is catalogued using a unique identifier, either choice could result in wide spread dissemination and linking of information about individuals.

### The Social Security Number

Almost all of the recent health care initiatives have proposed using the SSN as the unique personal identifier because it is viewed as providing the most cost effective and timely method of identifying the individual and reliably collecting and sharing personal information.

Both the Medical and Health Information Reform Information Act of 1992[9] and the Health Care Cost Containment and Reform Act of 1993[10] mandate use of the Social Security Number as the unique personal identifier. Although the Clinton Administration's Health Security Act left determination of what the unique identifier should be to the National Health Board which was created as part of the Act," the Health Information Privacy Survey sponsored By Equifax in 1993[12] reflected the public's support for use of the SSN as the identifier for a national health insurance program. Sixty seven percent (67%) of respondents would prefer it if their existing SSN were used rather than a new number developed just for national health insurance.

The SSN is commonly accepted as identification, and most United States citizens and residents have one. If the SSN is used as the unique personal identifier, no new identification number need be introduced nor dollars spent on generating and circulating a new number or on education for its use. The cost of verifying the identities of all holders and issuing a new, secure Social Security card is estimated in the $1.0 billion to $ 2.5 billion range. Supporters argue that this cost is far less than creating a new system. In spite of current problems, they believe the SSN can be verified corrected and validated more quickly and at less expense than creating a new system. [13] Moreover, check digits could be added to overcome current problems with the number's accuracy.

Organizations involved in developing computer based patient records have also recommended use of the SSN. The Computer-based Patient Record Institute "supports the immediate adoption of the SSN as the personal identifier with significant steps taken to overcome the criticisms -to its use. "[14] It further states that: "The overriding advantages to use of the Social Security Number, and the reasons for CPRI's support is economy. Minimal investment will be required to use an existing number, which many health care providers already collect and which has demonstrated success in one of the largest care systems in the U.S. " (Veterans Administration). [15] In its July 1992 report to the Secretary of the Department of Health and Human Services, the WorkGroup on Electronic Data Interchange (WEDI)[16] indicated that it "shall determine a process for a universal provider, subscriber and payer ID system by the fourth quarter of 1993, given limitations in current solutions. "[17] After much deliberation, WED1 now supports use of the SSN.[18] The Report of the WorkGroup on Computerization of Patient Records stated that setting up a patient identification code number to be used in electronic health record systems will need to be resolved early in the process of moving to such systems. While it discussed the issues, it deferred making a recommendation on what the unique identifier should be.[19]

Objections to the use of the SSN have been raised both on civil liberties grounds and because the SSN at present is not a completely reliable identifier: it is not unique, there are multiple users of a single number, and it is difficult to determine whether a random nine digit number is a valid SSN.[20] The Medical Records Institute has stated that opposition to use of SSNs as the unique identifier cannot be ignored.[21] It notes that: "Many of the people who oppose the introduction of the SSN as a universal identifier have had experience using them. Many private sector hospitals have used SSNs as unit numbers and have spent substantial funds to change from SSNs to true provider-based unit numbers. "[22]

The SSN is also used extensively for a large variety of nonhealth related purposes. The range of uses has grown steadily since 1936, as shown in Figure 4.1, which presents a chronological summary of changes in the use of the SSN by Federal agencies since it was created. The Office of Inspector General, Department of Health and Human Services in a recent report on the extent of use of SSNs, found that an overwhelming majority of public and private sector agencies in the United States use SSNs as a normal part of their operations.[23] They have stated that the widespread use of the SSN makes it increasingly critical that SSNs in organizational files be accurate."

Among the many non-Federal users of the SSN are debt collectors, department stores, utilities, check validation services, super markets, cable television, credit card issuers, banks, major oil companies, mailing list companies, credit bureaus, law enforcement agencies, insurance companies, hospitals and doctors, the Medical Information Bureau, motor vehicles departments, employers, schools and universities, and State agencies.[25,26]

Opposition to use of the SSN appears to arise from the fear that its use facilitates organizations' ability to link databases on many aspects of a person's life.[27,28,29] Individuals may fear that such information exchanges may not be beneficial to them and should not be encouraged.[30] If the SSN is used to facilitate uncontrolled exchanges of information, dossiers about individuals may be created which follow them throughout their life. "An individual's capacity to make a fresh start in life would be hampered, and the processes of social control of individuals would become increasingly threatening. "[31] At the same time, many people fear that the Social Security number has already become a ***de facto*** national identifier. [32]

Social Security numbers are used by many organizations to obtain information about individuals without their knowledge. While many of these enquiries are legal, they subject individuals to potential risks of harm without providing them with the knowledge necessary to protect themselves.[33] Evan Hendricks, in Testimony Before the House Committee on Ways and Means' Subcommittee on Social Security, stated:

> Not only does the SSN make it easier for large institutions to compare their databases, it allows curious individuals (including private detectives, computer hackers or other strangers you might not want snooping into your private lives) to "hop" from database to database and draw out a profile of your buying habits and personal lifestyle. The stranger might go to your Department of Motor Vehicles and get your SSN from your publicly available driver's license then using the SSN, he might, albeit illegally, go to a credit bureau and find out what debts you owe, go to an insurance company of the Medical

**e 4.1**

**Summary of Changes in the Use of SSN**

| DATE | AUTHORIZATION | USE OF SSN |
|---|---|---|
| **1936** | Social Security | Developed an enumeration system so that every person could be issued a nine digit Social Security Number (SSN) which would reliable distinguish his or her record of earning from all others. (Number was developed exclusively for internal use.) |
| 1943 | Executive Order 9397 | Authorized use of SSNs by an Federal agency establishing a new system of permanent numbers for internal employees. |
| 1961 | Public Law 87-397<br>IRS Code 6109 | Each tax payer required to furnish identifying number for tax reporting. |
| 1964 | Decision by SSA Commissioner | Assignment of SSNs to pupils in 9th grade and above. |
| 1965 | Executive Order 9397 | OPM includes SSNs on retirement record. |
| 1965 | Decision by SSA Commissioner | SSN issued to every old-age assistance recipient who didn't have one. This action was to allow for efficient exchange of information between State Public Assistance Agencies and SSA. |
| 1965 | Public Law 89-384 | Medicare enacted. It became necessary for most individuals 65 and older to have an SSN. |
| 1966 | Social Security | DVA began using the SSN as a hospital admission number. |
| 1966 | Decision by SSA Commissioner | Authorized Public Health Services Division of Indian Health to use SSNs to keep records of Indian beneficiaries of health services. |
| 1967 | Social Security | Department of Defense began using SSNs to replace Military Service Numbers and to report wages to SSA. |
| 1972 | Amendments to the Social Security Act | Mandates assignment of SSNs to individuals who are applicants or recipients of benefits under any program financed from Federal Funds. |
| 1972 | Amendments to the Social Security Act | SSA began issuing SSNs to children below school age when requested by parents or guardians. |

| DATE | AUTHORIZATION | USE OF SSN |
|---|---|---|
| 1974 | Public Law 93-579 | Federal, State and local agencies which request an individual to disclose an SSN shall inform the individual if disclosure is mandatory or voluntary (This is the first mention of SSN use by local government). |
| 1975 | Public Law 93-647 | Office of Child Support Enforcement Parent Locator Services may require disclosure of limited information (including SSN and whereabouts) contained in SSA records. |
| 1975 | Public Law 93-647 | Supplying one's SSN becomes a condition of eligibility for AFDC. |
| 1975 | Public Law 94-88 | Supplying SSNs of certain members of one's household becomes a condition of eligibility for Food stamps. |
| 1976 | Social Security Act Section 205(c) | State governments can use the SSN as an identifier for any tax, public assistance, drivers license or vehicle registration program. |
| 1976 | Tax Reform Act | States can use the SSN as an identifier for any General Public Assistance program under their jurisdiction. |
| 1983 | Public Law 93-67 | Provides for a monetary penalty for all who fail to furnish a correct tax identification number, usually the SSN. |
| 1984 | Public Law 98-369 | Requires applicants for AFDC, Food Stamps, Medicaid and Unemployment Insurance to furnish their SSNs for the purpose of permitting programs to use SSNs to associate records on individuals. |
| 1986 | Public Law 98-514<br>Tax Reform Act | Requires individuals filing a tax to include the taxpayer identification number (TIN) -- usually the SSN -- of each person age 5 or older whom the taxpayer claims as a dependent. |
| 1986 | Immigration Reform and Control Act | Establishes SSN card as evidence of employment authorization. Requires a study suing an SSN verification system to enforce employer sanctions. |
| 1987 | Decision by SSA Commissioner | SSA conducts an enumeration at birth pilot project which provides parents with a convenient way to secure SSNs for newborn babies. Project was later expanded nationwide. |
| 1988 | Public Law 100-647 | Established the Blood Donor Locator Service. It allows States to use SSNs to identify blood donor. |

> Information Bureauand find out about your health coverage and/or medical condition, check out various publishers to see what magazines you subscribe to and check with a few grocery stores trying out new computerized, "frequent buyer" programs to learn what your buying habits are. Access to credit bureaus is illegal, the laws are unenforced. There are few laws barring access to other private sector data bases.[34]

There are also clearly fraudulent uses of SSNs by organizations and individuals, both for their own purposes or to gain unauthorized second party access to information. In testimony before the Subcommittee on Social Security and Family Policy, the Deputy Inspector General for Investigations, DHHS, stated that the number of "information" brokers attempting to obtain, buy and sell Social Security Administration data to private companies, for their use in locating people or making decisions on hiring and firing, has expanded and that these brokers are increasingly turning to illegal methods for obtaining information.[35] While it is difficult to get exact information on these often covert or illegal activities, there is a growing body of anecdotal evidence being compiled by organizations such as the *Privacy Journal*, the *Privacy Times* and others attesting to their existence and significance to particular individuals.[36,37,38]

In recent testimony, Marc Rotenberg, Computer Professionals for Social Responsibility, described the black market in government data. He reported on two recent articles in the press about information brokers buying and selling confidential government records:

> Two months ago, *The Washington Post* reported that 16 individuals in 10 [S]tates were arrested in the largest case ever involving the theft of Federal computer data. So-called information brokers boasted that they could provide detailed personal information on anyone in the country. The records ranged from private credit reports and business histories to driver's license records, Social Security records and even criminal history backgrounds. These confidential records were taken from government agencies and sold for a fee to lawyers, insurance companies, private employers and others. Peter Neumann, a computer expert, said that "The public is abysmally uninformed about problems like this. With sufficient access to a few databases these days, you can get pretty close to somebody's life history with nothing more than a Social Security Number.
>
> A story in Time Magazine described 'a black market in government data' that included Social Security employees, police officers, private eyes and 'information' brokers. According to Time, Social Security employees sold earning histories for $25 apiece, and these were then marked up and resold by brokers for as much as $175. Even a top-ranked IRS criminal investigator was recently indicted for selling non-public material records to a California-based investigation outfit run by ex-IRS officials."

Mr. Rotenberg also reported that a sales brochure from Nationwide Electronic Tracking states, "with just a person's Social Security Number, Nationwide Electronic Tracking could provide name and home address (within l-2 hours for $7.50), place of current employment (1 week, $75), and previous employment and earnings (3-5 days, $100-$175)."[40]

In spite of examples where the SSN has been abused, the Commission and many others have pointed out that "...there is no evidence to suggest that any unique aspect of the Social Security number is peculiarly objectionable. Presumably, any other label -- except a name -- that is used as widely would arouse the same opposition and, if each individual had a unique name for life, used by him alone, it is conceivable that names would also become a target of concern."[41] There are risks involved in creating any specialized unique identifier since it is almost impossible to prevent Congress and the President from authorizing additional uses for the new number at a later date.[42] A new unique identifier for health could also serve as the basis for an ongoing enumeration of the U.S. population just as well as the SSN.[43]

**Other Options**

The alternative to using the SSN as a unique identifier is to create a new number. Some institutions have been working to find an alternative unique identifier to be used by the health care system.[44] In some cases, these efforts clearly fail to alleviate existing concerns as the SSN is embedded in many of the new numbering schemes being proposed. The Codes and Structures Work Group of the CPRI considered a new identification number which incorporated the SSN. In the end, however, they recommended use of the SSN. The American Society for Testing and Materials (ASTM) is considering a health insurance number consisting of at least 16 characters including a regional code, the SSN, a confidentiality code that could serve as a password for protecting specific files, a birth year code, and verifiers.[45] The Work Group on Electronic Data Interchange (WEDI) envisions that "in the future, a patient would be identified by biometric means (fingerprint, speech pattern, retina scan) and this identification would provide the basis to cross-reference an individual to an insurance number and/or a health record number."[46] Until then, they recommend use of the SSN.

A few organizations have proposed new numbers that do not incorporate the SSN. The AETNA Insurance Company uses a 17 digit number provided by the policyholder, who may select any elements that he or she wishes for inclusion. Many other organizations, such as the Harvard Community Health Plan, use a number other than the SSN as a patient identifier in automated records. Unless appropriate precautions are attached to this number, the ease with which health and nonhealth record systems could be matched is increased.

A recent Institute of Medicine report, *Health Data in the Information Age*,[47] carefully delineates six characteristics which the IOM believes are critical to any unique identifier. The number must be easily transitioned from the current system to the proposed health data organization and the physical structure of the number, i.e. number of digits, should be carefully considered to minimize repercussions on hardware and software. Error control features should be built into the number and system to prevent data entry mistakes, detect

errors, and correct mistakes. The system must be able to identify the person's identity and, under a separate process, verify that identification. The identifier must work anywhere a health service is rendered and must never impede access or delivery of health care. Similarly, the identifier must function anywhere in the country and in any provider office and must be able to link events occurring at multiple providers. Finally, the number, system, and process must minimize opportunities for crime and abuse, and if possible, identify perpetrators.

*DATA LINKAGES*

Of particular concern in attaching a unique identifier to a patient record is the ability it affords to link health related data with other kinds of data. There is a history of permitting new uses for the SSN, which when viewed one at a time, support important social purposes. However, they also provide the basis for building a comprehensive profile of individuals.

What appears to be most important, then, is to develop guidelines for linking data no matter what unique identifier is used. In its report, the Privacy Protection Study Commission recommended that development of a standard, universal label for individuals, or a central population register, should be deferred until such time as significant steps have been taken to implement safeguards and policies regarding permissible uses and linkages of records about individuals. [48]

Developing a new number and restricting its use to the health care sector would ensure that each person's health number would not be used for linking health and nonhealth information. In this case, the Social Security Number could not be an allowable data element in health care records, since its inclusion would make linkages with nonhealth records feasible.

Clearly, some linkages will be required to support public health, research and other socially important purposes. Many public and private agencies have defended the need for linking health records from many sources for research purposes. [49] In order to meet some research purposes, nonhealth data will also be needed so that the effects of life style, race and ethnicity, income, education, and other sociodynamic factors on health status can be evaluated. In most cases, these linked data sets can be structured so that individuals cannot be identified. In some cases, additional linkages might be necessary.

Canada has also addressed the use of the unique identifier for linking data sets. The Province of Ontario developed a separate medical identification number. Before the introduction of the new number, the head of the household had access to all family records because they were listed under his/her identification number. The new, unique number allows for the confidentiality of each person's record and is accompanied by guidelines for its use, including:

> . . .no person shall require the production of another person's health card or collect or use another person's health number; the number can only be used to provide

provincially funded health services and for “purposes related to health administration or planning or health research or epidemiological studies. "[50]

This legislation is sensitive to the need to restrict the use of health identifiers in both the public and private sectors in order to control violations of privacy and reduce public anxieties about the abuse of these numbers.

In developing this system, Ontario was responding to concerns similar to those expressed in the United States. Namely, "… that if not controlled the HN .. (Health Number). , could result in proliferating through society and becoming an unique personal identifier used to link data bases thus making it easier to not only collect more personal information in more data bases but increasing the capacity to conduct computer matches, create profiles and other usages, all of which could result in less privacy for the individual. "[51]

*SUMMARY*

Use of a unique personal identifier for medical records raises significant privacy concerns. While no decision has been made about which number will be used, decision makers are leaning toward the use of the Social Security Number. Proponents contend that it is the most cost effective approach to instituting a number in a timely fashion. Opponents argue that it is not unique and there is little or no security attached to its dissemination. Whichever number is chosen, attention must be paid to which data linkages will be permitted and for what purposes. The number chosen for an identifier must be developed and protected in such a way that the American public is assured that their privacy will be protected.

## *ENDNOTES*


1. Privacy Protection Study Commission. *Personal Privacy in an Information Society: The Report for the Privacy Protection Study Commission.* Washington, DC: U.S. Government Printing Office. 1977:605.

*2.* Privacy Protection Study Commission. 1977:607.

*3.* Privacy Protection Study Commission. 1977:610-611.

*4.* Privacy Protection Study Commission. 1977:608.

5. While particular groups vary in the specifics of their vision, those focusing on development of automated health care systems (e.g. the Computer-based Patient Record Institute, Medical Record Institute, and American National Standards Institute) envision a comprehensive longitudinal computer-based patient record containing all clinical, financial and research data; a "national" electronic network for accessing this health record for a variety of purposes such as primary care, insurance payment, peer review, cost containment, public health and research purposes; use of a smart card for purposes ranging from providing health insurance coverage information to providing a conception-to-death record of all health care; and use of unique patient-specific identifiers nationwide, and perhaps world wide.

---

6. Work Group on Computerization. *Toward a National Health Information Infrastructure: Reports of the Work Group on Computerization of Patient Records to the Secretary of the U.S. Department of Health and Human Services.* Washington, DC: USDHHS. April 1993:8.

*7.* Work Group on Computerization. 1993:15.

8. For statements of the benefits to be realized from development of computer-based patient record systems see: Dick RS, Steen EB. **The Computer-based Patient: An Essential Technology for Health Care.** Washington, DC: National Academy Press. 1991 and Work Group on Computerization. 1993. DHHS has also created the HHS Computerized Patent Record Council to coordinate departmental activities related to computerized patient records. (U.S. Department of Health and Human Services. *Initiatives Toward the Electronic Health Care System of the Future, White Paper.* Washington DC:Author. 1992.

*9. The Medical and Health Insurance Reform Information Act of 1992.* Legislation proposed by Louis W. Sullivan, Secretary of the Department of Health and Human Services. June 16, 1992.

10. *H. R.* 200: *Health Care Cost Containment and Reform Act of 1993.* 103rd Congress, First Session. U. S. House of Representatives. January 5, 1993.

11. H.R. 3600: American Health Security Act of 1993. 103rd Congress.

12. Louis Harris and Associates, Equifax Inc. ***Health Information Privacy Survey, 1993.*** ***New*** York, NY: Louis Harris and Associates. 1993. Study No. 934009.

13. King GS. ***Testimony by the Commissioner of Social Security. Testimony before the U.S. Congress, House Subcommittee on Social Security, Committee on Ways and Means.*** February ***27,*** 1991.

14. Computer-based Patient Record Institute. ***Position Paper: Computer-based Patient Records Standards. 1993*** : ***2.***

15. Computer-based Patient Record Institute. 1993 : 2.

16. Working Group on Electronic Data Interchange. ***Report to the Secretary of U. S. Department of Health and Human Services.*** Washington, DC: Government Printing Office. July 1992.

17. Workgroup on Electronic Data Interchange. 1992:Appendix 7.

18. WorkGroup on Electronic Data Interchange. 1992.

19. Work Group on Computerization. 1993:Appendix D, 15 and 16.

***20.*** Computer Professionals for Social Responsibility (Roberts E, Goldman J, Hendricks E, et al.): ***Letter to Hillary Rodham Clinton*** (Written communication, April 26, 1993).

21. Medical Records Institute. ***Toward an Electronic Patient Record: Updates on Standards and Developments, Analysis Number 2: Concept Models of Patient Identification, Issues Surrounding the Use of Social Security Numbers for Patient Identification***. Newton, MA: Author. 1993.

***22.*** Medical Records Institute. 1993:8. Some of the problems reported by private-sector hospitals in using SSNs include: over 10 million duplicates; several million people without SSNs (such as illegal aliens or young children); lack of flexibility due to the block structure of SSNs; and, error in data entry due to the lack of check digits and other security measures; See King. 1991.)

***23.*** U.S. Office of the Inspector General. The ***Extent and Use of Social Security Numbers.*** Washington, DC: US Government Printing Office. August 1988. Publication No. OAI-06-88-00800.

24. Inaccurate records could result in innocent individuals being subject to unwarranted intrusions into their privacy or to receiving improper treatment. They examined the degree to which verification of SSNs differed depending on the purposes for which they are used and concluded that, by and large, agencies are only slightly more careful when using SSNs for whom accuracy is important than when using them for other purposes (p. 10).

25. Smith RE. ***Report on the Collection and Use of Social Security Numbers.*** Providence, RI: Privacy Journal. 1985.

26. Hendricks E. ***Hearing on the Use of the Social Security Number as a National Identifier, Testimony before the U.S. Congress, Subcommittee on Social Security, Committee on Ways and Means.*** Washington, DC. February 27, 1991.

***27.*** Flaherty DH. ***Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.*** Chapel Hill: University of North Carolina Press. 1989: 1516,406.

***28.*** Flaherty DH. Privacy, Confidentiality, and the Use of Canadian Health Information for Research and Statistics. ***Canadian Public Administration.*** 1992;35(1):75-93.

***29.*** At least one author recommends that if social security numbers "are used in reports, they should be scrambled upon input, with the output key being strictly regulated." See: Bruce JAC. ***Privacy and Confidentiality of Health Care Information.*** 2nd ed. Chicago: American Hospital Publishing. 1988:63.

30. Marx GT. The iron fist and the velvet glove: totalitarian potentials within democratic societies. In: Short JE, ed. ***The Social Fabric: Dimensions and Issues.*** Beverly Hills, CA: Sage Publications. 1986.

***3 1.*** Privacy Protection Study Commission. 1977:610,611.

***32.*** This is not a new concern. The Social Security Number Task Force in it's ***Report to the Commissioner, Social Security Administration,*** May 1971, devoted a whole chapter to discussion of "The Trend Toward the SSN as Universal Identification Policy--Implications for SSA Policy."

33. Hendricks. 1991.

34. Hendricks. 1991.

35. Morey LD. ***Testimony of the Deputy Inspector General for Investigations, Department of Health and Human Services, Hearing before the Subcommittee on Social Security and Family Policy.*** Washington, DC. February 28.

***36.*** Smith RE, Siegel E. ***War Stories: Accounts of Persons Victimized by Invasions of Privacy.*** Providence, RI: Privacy Journal. 1990.

37. Rothfeder J. ***Privacy for Sale: How Computerization has Made Everyone's Private Life an Open Secret. New*** York: Simon and Shuster. 1992.

***38.*** Hendricks. 1991.

39. Rotenburg M. ***Testimony before the U.S. Congress, House Subcommittee on Social Security, Committee on Ways and Means.*** Washington, DC. February 27, 1991.

40. Rotenburg. 1991. The text of the brochure originally appeared in ***Harper's Magazine.*** March 1992:26.

41. Smith. 1990: 11. Smith states: "A small minority of persons object to Social Security enumeration on religious grounds. Many fundamentalist Christians point to the Biblical passage about a great beast that resembles Satan: "And he causeth all, both small and great, rich and poor, free and bond, to receive a mark, or the name of the beast, or the number of his name. And than no man might buy or sell, save that he had the mark, or the name of the beast, or the number of his name.. . .And the third angel followed them, saying with a loud voice, If any man worship the beast and his image, and receive ***his*** mark in his forehead, or in his hand, the same shall drink of the wine of the wrath of God,. . .and he shall be tormented with fire and brimstone." (Revelation 13:16-17 and 14:9-10.) Files of the Social Security Administration and ***Privacy Journal*** include complaints based on the Biblical passage, which some preachers say instructs believers to shun all enumeration by the federal government beast.

42. Flaherty D. ***Ensuring Privacy and Data Protection in Health and Medical Care.*** Paper presented to the Kennedy Center on Ethics, Georgetown University. April 1993.

***43. See*** materials prepared by the Department of Commerce Task force for Designing the Year 2000 Census and Census Related Activities for 2000-2009.

***44.*** Carpenter PC, Chute CC in an unpublished manuscript from the Mayo Clinic suggest using a geographic code based on the latitude-longitude grid, a sequence code for persons born on the same day and a check digit. The American Medical Record Association/American Health Information Management Association based a proposed unique identification number based on the Mayo manuscript.

***45.*** Elmer R. Gabrielle, M.D. the Health Care Vice-Chairman of Committee E-3 1 on Computerized Systems has been circulating in draft "A Guide for the Development of a Universal Healthcare Identifier." This proposal is under consideration within an ASTM Technical Committee as an ASTM Standard, but it has not received all of the approvals required to become an ASTM Standard.

***46.*** Medical Records Institute. Health care networks. ***Toward an Electronic Patient Record.*** Newton, MA: Author. April 1993;1:9.

47. Institute of Medicine. ***Health Data in the Information Age: Use, Disclosure, and Privacy.*** Donaldson MS and Lohr KN, eds. Washington, DC: National Academy Press, 1994.

***48.*** Privacy Protection Study Commission. 1977:637.

49. Agency for Health Care Policy and Research. ***The Feasibility of Linking Research-Related Data Bases to Federal and Non-Federal Medical Administrative Data Bases, Report to Congress.*** Washington, DC: Author. 1991. U.S. Department of Health and Human Services Publication 91-0003.

***50.*** Bill 24 was introduced by the Ontario Minister of Health to "control the private use of cards issued and numbers assigned to insured persons under the Health Insurance Act. " These guidelines are found in Section 2( 1).

***5*** 1. Reily T. ***Ontario's Health Number: Handling the Privacy Threats, A Report for the Client Services Branch, Ministry of Health.*** Kingston, Ontario: Riley Information Services Inc. 1993.

## *DEVELOPMENT OF A PZUVACY ENTITY*

### *INTRODUCTION*

As medical records are transformed from paper documents into data bits transmitted over electronic networks, the risks to the privacy of the individual are changing. This dramatic change in how information is collected, stored, and used requires consideration of the need for an entity at the Federal level to address, in a systematic fashion, the privacy issues. This section focuses on the history and present status of efforts to develop some form of privacy entity at the Federal level, activities in other countries, the arguments for and against the development of such a body, and the role and functions of such an entity.

### *BACKGROUND*

**Privacy Protection Act and Study Commission**

The establishment of a Federal Privacy Board with regulatory powers over the private sector was proposed as an integral part of the Federal Privacy Act bill introduced by Senator Sam Ervin in 1972.' However, it met with opposition from the Ford Administration and the Privacy Act of 1974, as ultimately enacted, created instead a time limited study body, the Privacy Protection Study Commission (PPSC).[2]

The PPSC in turn recommended that an "independent entity within the Federal government"[3] be established to perform four ongoing functions:

- Monitor and evaluate statutes and regulations enacted by Federal agencies to protect privacy "and have the authority to formally participate in any Federal administrative proceeding or process where the action being considered by another agency would have a material effect on the protection of personal privacy, either as the result of direct government action or as a result of government regulation of others" .[4]

- Conduct research and investigate citizens concerns regarding privacy in both the public and private sector.

- Issue rules that must be followed by Federal agencies interpreting the Privacy Act of 1974 or revisions thereto.

- Advise both the legislative and executive branches of government regarding the privacy implications of statues or regulations, and when requested, advise States regarding the privacy implication of proposed Federal or State regulations or statutes.

The Commission recommended that this entity have some enforcement authority over Federal agencies with respect to their responsibilities under the Privacy. Act of 1974, but did not

include the private sector within the scope of its regulatory role. It did, however, recognize a Federal responsibility to identify privacy abuses in the private sector and recommend changes.' The recommendations were never implemented but the concept of an oversight privacy protection body has been proposed repeatedly over the years. Several States, including Hawaii, Minnesota, and Wisconsin have recently established data protection boards to govern the public sector, but the private sector has been virtually unregulated.

**Legislative Proposals for a Data Protection Board**

More recent legislative efforts to establish a permanent privacy oversight entity at the Federal level have been proposed; they received little attention and none have resulted in legislation. Congressman Glenn English offered bills in the 98th and 99th Congresses[6] to create such a body, and similar proposals were offered by Congressman Robert E. Wise in the 101st and 102d Congresses.[7] These proposals would have established a board or commission (the precise name varied in the several proposals) to perform essentially the functions outlined by the Privacy Protection Study Commission in 1977. The board would supervise Federal compliance with the Privacy Act, and assist the private sector in developing data protection standards. It would not have had regulatory authority over the private sector. This board was intended to address private citizens' concerns with data collection and record keeping practices by serving as an advisory and review committee on matters relating to data protection and standards and fair information practices. It would have had the power to "accept and investigate complaints about violations of data protection rights and fair information practices, " thus providing citizens a mechanism other than judicial proceedings, to have their complaints heard.

These proposals were viewed by many as providing the "missing piece" in addressing activities that undermine or threaten privacy standards. The board would have encouraged voluntary compliance with privacy standards within both the federal government and private industry.[8] It was also seen as the vehicle for promoting the adoption of Fair Information Practices on a more widespread basis. These proposals would not have given the board direct enforcement powers within the Federal government (like commanding an agency to take or not take some action). Some, including Mark Rotenberg, testifying in 1990 on H.R. 3669, for Computer Professionals for Social Responsibility, believed that the Board should have such enforcement powers to enable it to function effectively.' With respect to the private sector, the Direct Marketing Association argued that self regulation was far more acceptable to the private sector than mandatory legislation and testified that many marketers already voluntarily inform consumers of their practices. In a presentation to the HHS Task Force, Mr. Rotenberg reiterated the value of a Data Protection Board, proposing that it could address the exchange of personal information among private sector companies and between the Federal and private sectors. If vested with enforcement powers, at least in the Federal sphere, it could address issues such as the secondary use of data."

Concern on the part of privacy protection advocates was based on the weakness of the proposed entity, and the fact that it did too little to control private businesses. Evan Hendricks of the Privacy *Times* feared that the board's proposed powers were deficient. In

addressing H.R. 685, he called on Congress to "advance the laws to keep pace with technology" and supported a government wide data protection board as well as separate agency boards to oversee data integrity and privacy measures within the government. [11]

On the other hand, private business interests such as the direct marketers, felt that the bill was too strong, too threatening, and bordered on regulatory intervention. Others commented that a lone Federal board or commission is not sufficient and that State agencies could also be created and even partially funded by the Federal entity to investigate citizen complaints. The Federal entity's responsibilities to inform the public of its privacy rights could be extended by State agencies.

These proposals for a board received little attention. Mr. Wise, the Chairman of the Government Information, Justice, and Agriculture Subcommittee of the House Government Operations Committee, held a hearing in 1990 which included testimony on the board proposal (including some of the comments described above), but no further action occurred.

**Efforts under the Bush Administration**

In November, 1991, **the** Secretary of HHS convened a forum of health care leaders to identify ways to reduce health care administrative costs. As a result of the forum, four work groups were created to discuss technical and policy issues. One group, the Work Group on Computerization of Patient Records, produced a report that included a recommendation for a privacy body (as well as a recommendation for Federal preemptive health record privacy legislation). It recommended a Federal Information Privacy Commission as "part of the national information infrastructure that would establish uniform requirements for protecting the confidentiality of health information and potentially, other types of information (e.g. credit, personal finances). " The Commission would be appointed by the President and would represent patients, providers, payers, researchers, other Federal agencies, and other interested parties. It would have regulatory powers and would be responsible for implementing and enforcing Federal legislation. [12]

**Health Care Reform**

The Clinton Administration's proposal for reform of the health care system, the Health Security Act[13], included provisions for an advisory committee to address data and privacy issues regarding health records. The bill included administrative simplification and standardization activities with regard to health care information about individuals, and had some provisions relating to confidentiality of this information. The bill would have established a National Privacy and Health Data Advisory Council to advise the agency administering the program, the National Health Board, on privacy and data issues. It proposed a membership that included, inter alia, individuals "distinguished in the fields of data collection, data protection and privacy, law, ethics, medical and health services research, public health, and civil liberties and patient advocacy. "[14] This was to be an advisory committee to a Federal agency, and it would have had no independent power.

**Senator Simon's Proposal**

The most recent effort was Senator Paul Simon's proposal in 1993 for establishment of a Privacy Protection Commission.[15] This proposal was similar to the House bills. It would have created a five person United States Privacy Commission with a series of leadership, guidance, and advisory functions. It would have overseen Federal agencies' implementation of the Privacy Act, but would not have had authority to order a Federal agency to act. Again, there would be no regulatory function with respect to the private sector, although the bill envisioned assistance to the private sector in the development of confidentiality policies. The bill received some attention, but was not enacted.

**Public Attitudes and Views**

The Equifax Report on Consumers in the Information Age (1990) reported on a national opinion survey (conducted by Louis Harris and Associates and Dr. Alan Westin) that included questions on a public privacy body.[16] The survey included interviews with 2,254 Americans eighteen years of age and older (public), and 916 corporate executives ("leaders", in the survey's parlance) from insurance companies, consumer credit grantors, banks and thrifts, direct marketing organizations, human resource firms and consumer affairs companies. Respondents sampled in the public and the leaders groups were presented with three options for what is needed at the Federal level to protect consumer privacy:

- Stay with the present system of specific laws, congressional oversight, and individual lawsuits;
- Create a nonregulatory privacy protection board to research and publicize new controversies over privacy for public policy considerations; and
- Create a regulatory privacy protection commission with powers to issue enforcement rules for businesses handling consumer information.

Results of the survey indicate that among the public, 41% believe a privacy commission with regulatory powers to enforce rules should be established, 31% think the country should stay with the present system, and the remaining (24%) think a nonregulatory privacy board would be beneficial.

Consumer affairs executives were evenly divided among the three choices while executives in privacy intensive industries (credit- 55 % , human resources- 51% , insurance- 49 % , banks and thrifts- 43 % , and direct marketing- 39 %) were in favor (majorities or pluralities) of keeping the present system.

In a later survey focused on health information within a framework of national health care reform, the 1993 Equifax Health Information Privacy Survey,[17] 86% of the public (N = 1000) and 69 % (N = 65 1) of the "leaders" thought it important that "an independent National Medical Privacy Board.. . be created.. ." to hold hearings, issue regulations, and enforce standards as part of a new Federal confidentiality law. The leaders interviewed include chief operating officers of hospitals, health maintenance organizations and health

insurers, physicians, nurses, medical society heads, State regulators, State legislators, Congressional aides and human resources executives.

**Presentations to the Task Force**

In 1992-1993, the Task Force heard from a wide array of private sector organizations on the need for data to meet a variety of legitimate needs and on the importance of protecting individual privacy. While a wide variety of issues and needs emerged, many recommended the formation of a data protection board. Privacy advocates stated the need for a data protection board to oversee Federal and private sector data collection efforts and to enforce Federal or State mandates.'* Legal representatives saw the need for a data protection board to assist in overriding State laws and to serve as a "voice of authority. "[19] Statements from representatives of the insurance field supported the model law proposed by the National Association of Insurance Commissioners (NAIC).[20] Representatives from the technical arena, professional associations, and the media also supported a data protection board.[21]

*ACTIVITIES IN OTHER COUNTRIES*

The United States is not alone in its efforts to design organizational structures to ensure effective consideration of privacy values in public and private decision-making. Other industrialized nations are grappling with many of the same issues and their approaches offer alternatives for organizing privacy protection agencies. Several nations have implemented health and medical information practice boards at various organizational levels, including at site specific locations such as hospitals, as well as in national and sub-national regulatory agencies. Privacy protection boards that exist or have been proposed in America usually extend to only the public sector, while European boards protect both public and private sector health-related data. Some data protection boards have only advisory powers, while others have licensing and regulatory authority.

The European community (EC) and the Council of Europe, at a meeting in Luxembourg on access to public information, data protection and computer fraud, advised participants that the countries which do not develop data protection laws by 1992 might face problems in transborder data flow[22] that could possibly effect their ability to be competitive in the global economy. The development and implementation of an entity that could monitor, advise and enforce privacy protections would be an asset in satisfying the requirements of the EC.

**Canada**

The Federal Privacy Act of 1982 went into effect in July of 1983 and regulates the collection and use of personal information by the Federal government. The law established an official, the Privacy Commissioner, to monitor Federal agencies' implementation of the Act who has considerable investigatory and auditing powers. The Privacy Commissioner, appointed by and accountable to Parliament, monitors the Federal government's collection, use, and disclosure of its clients' and employees' personal information, and its handling of individual's requests to see their records.

The Privacy Commissioner does not enforce the Privacy Act; enforcement is carried out by the Trial Division of the Federal Court of Canada. However, the Commissioner reviews complaints and decisions which may be taken to court regardless of whether or not the Commissioner's decision is favorable to the complainant. The power of the Commission is limited to such an extent that it may not investigate the activities of an agency without first notifying that agency.[23]

Ontario and Quebec have been most aggressive in their approach to data protection. Ontario has had an Information and Privacy Commissioner since 1987 whose task it is to guide the implementation of legislation for the public sector. While the office has not succeeded in obtaining sectoral data protection legislation for medical and health information, it has conducted studies and given advice on a number of health related issues, including the dissemination of AIDS data, use of facsimile transmissions, and smart card technology.[24]

Quebec has had a privacy protection authority for more than a decade. In April 1992, it issued a set of minimum requirements for the security of computerized health records, acknowledging that "the possibilities for processing, linking, and matching data are virtually unlimited, and that [this] is where the main threat to confidentiality lies. "[25] The Commission advised that a record number for a patient, combined with the name of the establishment, should be considered identifiable personal information and further, that a responsible keeper, with the assistance of a committee, be appointed to implement and enforce security measures. In legislation effective on January 1, 1994, Quebec was the first Canadian province to extend its privacy protections to the private sector.[26]

**Germany**

The Federal Data Protection Act (BDSG) became effective for the Federal and some private sectors in January, 1973. States that did not already have a general data protection law enacted one soon after the this law. The German model is decentralized and consists of a Data Protection Commissioner at the Federal level. Each State has primary responsibility for health matters and has a counterpart to the Federal Commissioner. By advising the Federal government and individual ministers, the State level Data Protection Commission ensures that the Data Protection Act is implemented and that statutory requirements are followed. The State level boards implement both the Federal law and their complementary State laws. The practice of privacy protection, in summary, consists of lodging complaints with appropriate agencies regarding activities which the Commissioner views as violations of Germany's equivalent of the Privacy Protection Act.[27]

**Sweden**

The Data Act of 1973 was enacted to prevent "undue encroachment" on individual privacy. This law created the Data Inspection Board (DIB) to regulate the collection, storage and dissemination of identifiable personal data held in computerized form by either the public or private sectors. The law also provides civil and criminal penalties for violation of the Data Act. The Data Act was revised in 1982 to create a more permissive system and relieve an administrative logjam in approving data systems. The DIB is an independent authority whose

members are appointed for fixed terms and represent various political parties and interest groups. The staff is organized to specialize in types of information systems rather than industries. The licensing and supervisory functions coexist within the DIB's departments which handle either government or private systems. Licensing is the major activity and takes precedence over inspection and surveillance activities.

The Data Inspection Board is instructed to pay special attention to the nature and quality of the personal data being collected, how and from whom the data are being acquired, and the attitudes of the data subjects. In order to start or maintain a database of personal information, it is necessary to obtain permission and a license from the DIB, but the Cabinet or the legislature has the power to create a database without approval of the DIB. Once the data have been collected, the DIB has control over the dissemination and uses of the resulting register, and is responsible for enforcing a system of responsible keepers for computerized data banks. The DIB is reluctant to approve data system usages and is concerned about new applications of the existing system. It therefore tends to permit a specific use rather than grant a blanket license to a system.[28]

**France**

The French law of 1978 on Informatics, Data Banks and Freedoms created the National Commission on Informatics and Freedom (CNIL) and separate subcommissions on freedom to work, research and statistics, local government, and technology and security. The CNIL is composed of three executive officers and fourteen additional members who serve as commissioners. The commissioners represent the highest levels of public and private organizations in France. They serve five year terms, have regulatory and licensing authority, and make decisions on the authorization of particular information systems in response to requests from both the public and private sector.

The CNIL has not been as effective as many had hoped. The Commissioners do not devote their full time to the Comrnission and the majority are not professional experts in privacy law, informatics or other core activities of the CNIL. The requirements of the law and absence of local or State authorities place an impossible workload on a national staff that must somehow function without focused or consistent leadership.[29]

*SUMMARY*

Interest in a data protection board has waxed and waned for the twenty years since the Privacy Act first proposed its existence. A natural distrust of bureaucratic structure, the financial costs of a board, and a low level of public concern over privacy protection have acted as barriers to the establishment of such a board.

As a result, the United States has not created permanent oversight bodies in the data protection field to carry out the variety of activities necessary to ensure attention to privacy in design and management of data systems: give expert advice, promote fair information **practices, receive and investigate complaints, advance and facilitate access rights, conduct**

systematic audits and investigations of particular information systems, and report periodically on problems and progress.[30] However, as changes occur at an increased pace and automation is introduced on a widening scale, it becomes clear that additional formal mechanisms are needed to assess the new uses of transactional data. This points to the development of a data protection board to address the many privacy concerns that are emerging.

Increasingly, information is being shared across the Federal government, between public and private organizations, and among private organizations. Partly as a result of automation, organizations are increasingly doing business across State lines. Laws that were formulated to address Federally held health records do not apply to data held in the private sector which may receive no protection at all. Individuals now carry the burden for identifying improper data collection, data uses and users and for resolving the problem. At present in the United States, perceived violations of personal privacy can only be addressed by litigation by an individual, a process that is time consuming and often prohibitively costly. This creates monetary burdens which often discourages the individual from pursuing his/her complaint. In addition, this individual approach to addressing violations often fails to identify the systemic problems and abuses that exist. A data protection authority would serve as the arbiter in data issues related to privacy and confidentiality.

Privacy violations in arenas other than health care have raised public knowledge of and concerns with the confidentiality of health information. Anecdotal evidence of the abuses associated with records of cable subscribers' service and viewing habits, electronic mail, library borrowing customs and selections, video rentals, and criminal history files[31] have raised the public's consciousness and awareness of the danger of such invasion of privacy. Automation of information makes it possible to access a great deal of data in a short time from many locations.

As the health care system takes new organizational forms, and health records are increasingly automated, the challenge of providing total access to information about the performance and quality of care given by health care providers while protecting the privacy of patients suggests that a combination of strategies and organizational arrangements is needed. The need for accountability to the public at large and to the Congress is an argument for a single responsible group, a data protection authority. The success of the United States in competing in the international arena may well be related to its effectiveness in developing and implementing data privacy and security standards, as discussed above. At present, the U.S. lags behind other countries in protecting its citizens. Data protection authorities have been in operation in other countries for more than a decade. Establishing such an authority would enable the U.S. to continue the flow of transborder exchange of personal information.[32]

## *ENDNOTES*


1. S. ***3418,*** 93d Cong., 2d Sess., tit. I (1974).

***2.*** Albinger S. Personal information in government agency records: Toward an informational right to privacy. I986 ***Annual Survey of American Law.*** 19XX:625,642n. 150.

3. Privacy Protection Study Commission. ***Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission.*** Washington, DC: Author. 1977.

4. Privacy Protection Study Commission. 1977:37.

5. Privacy Protection Study Commission. ***Final Recommendations of the Privacy Protection Study Commission.*** Washington, DC: Author. 1977.

6. H.R. 3743, 98th Cong., 1st Sess. 1983.; and H.R. 1721, 99th Cong., 1st Sess. 1985.

7. H.R. 3669, 101st Cong, 1st Sess. 1989.; and H.R. 685, 102d Cong., 1st Sess. 1991. Introduction statement on latter bill at 137 Cong. Rec. H755, daily ed. Jan. 29, 1991.

8. Brennan T. Congressman calls for data board to monitor privacy; DMA Objects. ***DM News.*** May 28, 1990.

9. Rotenberg M, Culnan MJ, Rosenberg R. ***Hearing on Computer Privacy and H. R. 3669, The Data Protection Act of 1990, Testimony before the U.S. Congress, Subcommittee on Government Information, Justice and Agriculture, Committee on Government Operations.*** Washington, DC: House Committee on Government Operations. 1990.

10. Rotenberg M. ***Presentation to the Task Force on the Privacy of Medical Records.*** Washington, DC. February 18, 1992.

11. Quindlen TH. Congress pushes SSA on data security; U.S. Social Security Administration. ***Government Computer News.*** March 16, 1992.

12. Work Group on Computerization of Patient Records. ***Toward a National Health Information Infrastructure: Report of the Work Group on Computerization of Patient Records to the Secretary of the U.S. Department of Health and Human Services.*** Washington, DC: USDHHS. 1993.

13. H.R. 3600, 103d Cong., 1st Sess. 1993.

14. § 5140.

15. S. 1735, 103d Cong., 1st Sess. 1993.

16. Louis Harris and Associates and Alan F. Westin, Ph.D. conducted this survey for Equifax in 1989. Louis Harris and Associates. The ***Equifax Report on Consumers in the Information Age.*** Atlanta, GA: Equifax Inc. 1990.

17. Louis Harris and Associates, Westin AF. ***Harris-Equifax Health Information Privacy Survey 1993.*** Atlanta, GA: Equifax Inc. 1993. Leaders include executives, professionals and state and federal officials in the health care field (101 hospital CEOs, 50 HMO CEOs, 31 commercial health insurer CEOs, 100 physicians, 50 licensed registered nurses, 50 heads of state and national medical societies, 30 state health care regulators, 68 state legislators who serve on health care committees, 70 aides to federal legislators on health care committees, and 101 human resource executives).

18. The Privacy Advocates included: Evan Hendricks, Editor of Privacy Times; Marc Rotenberg, Director of Washington Office of CPSR; Michele Zavos, AIDS Coordinating Project (ABA); Peter Hawley, M.D., Medical Director of Whitman Walker Clinic; William Pierce and Mary Beth Seader of the National Committee for Adoption.

19. The Legal Arena included: Ron Plesser, of Piper & Marbury; and Robert Gellman, Chief Counsel, Subcommittee on Government Information, Justice & Agriculture.

***20.*** The Insurance and Credit Arenas included: Otto Meletzke, Senior Counsel, American Council of Life Insurance; and John Baker, Senior Vice President of Equifax.

21. The Media Arena included: Paul McMasters, Vice President of Freedom Forum. The Professional Organizations included; Margaret Amatayakul, Interim Executive Director, CPRI; Betty Fuchs, Project Director, JCAHO; Donna Pickett, American Hospital Association; The American Dental Association; Dr. Barbara Heller, American Nurses Association; The American Pharmaceutical Association; and E. Harvey Estes, Ethics and Health Policy Council, AMA. Technological Arena included Vincent Brannigan, Professor, University of Maryland and Dr. Bemdt Beier, Germany.

***22.*** Rotenberg M. ***Computer Privacy and H. R. 3669, the Data Protection Act of 1990.*** Washington, DC: Author. 1990: 17.

***23.*** Flaherty DH. ***Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.*** Chapel Hill, NC: University of North Carolina Press. 1989.

24. ***Annual Report, Privacy Commissioner, 1992-1993.*** Ottawa, Ontario: Canada Communication Group. 1993.

25. Commission d'Acces a l'Information. Minimum requirements for the Security of Computerized Records of Health and Social Services Network Clients. Quebec, Canada. April, 1992.

26. Personal correspondence with David Flaherty, Information and Privacy Commissioner, British Columbia. October 5, 1993.

27. Flaherty. 1989.

28. Flaherty. 1989.

29. Flaherty. 1989.

30. Flaherty. 1989.

3 1. For example, see “National Crime Information Center, Legislation Needed to Deter Misuse of Criminal Justice Information, " testimony of Laurie E. Ekstrand, United States General Accounting Office, before Subcommittee on Information, Justice, Agriculture, and Transportation, Committee on Government Operations, and Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, U.S. House of Representatives, July 28, 1993.

32. Rotenberg. 1990: 17.

## *INTRODUCTION*

Education and training are needed by those who are entrusted with health information. Those furnishing this information must also be educated regarding their rights and responsibilities. Among the many organizations and individuals who require education and training describing their rights and responsibilities either as providers or users of health information are:

- health practitioners who provide direct patient care and collect data while providing medical services, usually on a one to one basis;
- people who provide health related services including health and life insurers, medical researchers, and hospital administrators who collect either first or secondhand data and use this health information for payment for services, quality of care review, research and administrative control;
- organizations and institutions which do not provide health related services, but which collect personal health information in the course of everyday business, (i.e., credit corporations, employers, educational institutions, etc.); and
- the public who is asked to provide and disclose personal data to these organizations in the course of daily life, often to receive benefits or services.

Education and training are distinct but complimentary in that *education* is a means of imparting information on a subject and *training* is a means of putting into practice what was learned through education.' Those with access to identifiable data need to understand their obligations in preventing breaches of confidentiality, poor security practices, fraud or abuse. The public must also be made aware of its rights, understand the consequences of consenting to the disclosure of personal information and be aware of legal protections and the redress available to an injured party. Recently, the Computer-based Patient Record Institute (CPRI), Workgroup on Electronic Data Interchange (WEDI), Institute of Medicine (IOM) and the Work Group on the Computerization of Patient Records have all proposed making education and training available to suppliers and users of health information as an effective means of enhancing privacy. This section describes the target audiences for education and training and the approaches to providing these services being employed by various organizations.

## *BACKGROUND*

Organizations using health data often have programs focusing on safeguarding information under their control. However, it is difficult to quantify the number of organizations doing so or to determine the quality of education or training. Providers of health care, institutions, and organizations which access and use health care data and consumer oriented organizations are

increasingly offering training and education programs. Hospitals, physician offices, and other health care facilities providing direct health care services frequently offer at least a minimum of privacy and confidentiality education and training for their employees. They also offer information to their patients concerning their privacy protection policies and the rights of patients, often as part of obtaining permission to release information for third party payment.' However, some privacy advocates and bioethicists feel that these policies are more for purposes of protecting the institution rather than from any real concern for protecting personal privacy. [3]

Other private sector organizations who access, maintain, and disclose health information, but do not provide direct health care, have also developed education and training curricula for their employees.[4] These organizations may also make information about their privacy protection practices available to those for whom they provide services. This information may explain what protections exist, how the public can access information, and how confidentiality procedures are implemented.

Still other organizations inform consumers about current trends in the collection and use of health information and of their rights and responsibilities. The American Civil Liberties Union (ACLU), Computer Professionals for Social Responsibility (CPSR), the Public Citizen, Privacy International and the Public Voice, to name a few, address privacy issues from the public's perspective. There are also publications, such as, ***The Privacy Times*** and the Privacy ***Journal*** which inform the public of developments in privacy legislation, technological advancements and their effects on confidentiality, and programs and procedures implemented to protect privacy. These journals also publicize the "privacy horror stories" of private individuals and make the public aware of relevant issues.[5]

Advocacy and public interest research groups, like those identified above, attempt to provide the public with information that will help individuals make informed decisions about the health data they release. Advocates from these groups represent the interests of the individual by testifying at legislative hearings, serving as witnesses for judicial proceedings, and participating in policy making efforts. Through such organizations, new legislation and regulations, data collection efforts and research, and the latest technological advances are made known to the public. These organizations also voice public concerns to the appropriate legislative bodies. These groups maintain, as many others do, that individuals who understand how personal health information can be used will be better prepared to cope with improper use. They will be better able to correct the resulting problems and will learn when to withhold information that is not essential to disclose. Moreover, individuals who are educated about the use of health information will be more likely to cooperate with research and similar socially important activities.

### *TARGETS OF EDUCATION AND TRAINING*

Education and training programs which inform organizations and individuals of their responsibilities, appropriate data protection procedures, and penalties for misconduct may

contribute most to protecting privacy and confidentiality.[6] While health care professionals have adopted ethical codes that address their responsibility toward protecting client privacy, many people who collect or access patient's health care information are not health care professionals. Unit clerks, admission clerks, unlicensed assisting personnel, information systems staff, billing staff, third party payor clerks, and many others do not have formal codes of ethics to guide them in making decisions about patient information or to alert them to their responsibilities to protect the patient.' The pubic must also be made aware of its rights and responsibilities.

**Educating Health Care Professionals**

Educating health care professionals is central to any privacy protection strategy. [8] Most professional associations have "codes of ethics" designed to ensure that health professionals act responsibly in matters of patient care privacy and confidentiality while some also have "bills of patient rights. "[9] The manner in which education and training are addressed varies. Professional codes of ethics, proposals for model legislation, and guidelines for practice serve as approaches to educating and training health care professionals. For example:

- **The American Dental Association's (ADA)** ***Principles of Ethics*** and Code ***of Professional Conduct*** inform dentists of their ethical obligation to safeguard the confidentiality of health information; maintain patient records in a manner consistent with the protection of the welfare of the patient; and with permission of the patient, provide any information that will be beneficial for the future treatment of that patient. The Code also outlines sanctions and penalties for privacy violations. [10]

- Guidelines developed by the **American Hospital Association (AHA)** include a discussion on education which states that the hospital should establish rules for the use of medical records in hospital approved education programs for medical and health care professionals and should disseminate the rules to the appropriate program directors and instructors, who also must share the responsibility for protecting the confidentiality of the medical records and ensuring the availability of the records for patient care purposes. [11]

- **The American Medical Association (AMA)** model State legislation on confidentiality of health care information does not include provisions regarding education or training. However, a provision of the model act sets forth requirements for third parties receiving and retaining an individual's confidential health care information which mandates that these parties educate their employees and agents about sensitivity of data and proper use, storage, and disclosure of personal information. It also requires that third parties be made aware of penalties for breaches in security and a statement of receipt of information be signed. [12]

- The **American Nurses Association (ANA)** recognizes that "...there needs to be ongoing education to all staff regarding the need to limit indiscrete and unwarranted revelations related to specific patients.. ."[13]

- The **American Pharmaceutical Association (APhA)** ***Code of Ethics*** is an educational tool to guide pharmacists' professional relationships. It sensitizes and educates members on the importance of confidentiality in their practice.[14]

- The **American Psychiatric Association (APA)** educates members through a publication entitled ***Guidelines on Confidentiality,*** which was derived from its Code of Ethics. The document furnishes guidance on confidentiality and records maintenance, access, redisclosure, and release to third parties.[15]

**Educating and Training Employers and their Employees who Handle Health Information**

Some institutions provide educational and training seminars to employees on maintaining, using, and disclosing health information. While these efforts may add to costs, they provide benefits to both employer and employee that may, in the long run, outweigh any financial burden.[16] They contribute to improved client relations and may reduce employer liability in the event of a privacy violation. Education and training programs provide:

- a forum to present and fully explain the ethical and legal aspects of data collection and disclosure, the legal responsibilities of all concerned parties, and the opportunity for employees to discuss and sign nondisclosure agreements;

- an arena for the employer to clearly define terminology including delineating what is and is not considered confidential and when releases are needed, so that the employee will understand the ramifications of disclosure of personal data;

- a medium which allows the employer and employee to build open communication and an enhanced working relationship based on expectations of not only each other, but the patient or client as well; and

- an opportunity for the technical and personal skills needed to protect privacy and confidentiality to be taught.

In 1985, the **American Health Information Management Association (AHIMA),** formerly the American Medical Record Association (AMRA), which is the association for credentialed professionals in the field of health information management, published ***Confidentiality of Patient Health Information.***[17] ***This*** document sets forth Association policy regarding confidentiality and includes references to education for employees and the public. It states, "all health care personnel who generate, use, or otherwise deal with patient specific information should uphold the patient's right to privacy." It defines the model policy which

includes sanctions and a model employee nondisclosure agreement, and further states, "…because current philosophy places new emphasis on patient involvement in health care, providers have assumed active roles as educators so that the patient may be an active participant in the health care team. Health information managers must take a further active educational role in the creation of accurate records, and the establishment and exercise of individuals' information rights are primary areas for educational effort."

The **Direct Marketing Association (DMA),** a professional trade association, educates its members on the value of self regulation. Using personal information protection guidelines, the DMA has developed a "fair information practices checklist" which is designed specifically for member companies to use as an internal audit. The checklist is comprised of steps a company can take to ensure that consumer expectations for privacy are met. Inherent in the DMA's approach is the belief that companies "have a responsibility to train their associates in fair information standards" and that the use, and particularly the transfer, of sensitive health data be kept to a minimum. Consumers, according to DMA, must be empowered and companies have an obligation to provide their customers with educational information to show how they can protect health care data.[18]

The **Medical Information Bureau (MIB)**, a nonprofit association, provides its members (life insurance companies) with confidential information about the health of prospective insurance consumers to help insurance companies evaluate applicants. After much criticism in the 1970's, the MIB has developed public education materials and provides information to any individual in the public upon request concerning its activities, whether it maintains a file on him or her, what information is contained in the file, how the individual can access the file, and who has requested information from the file."

**Educating the Public**

In general, the public is not well educated about how health information is used or about their rights and responsibilities with regard to their information. While institutions often obtain the individual's consent before collecting and/or releasing information, this consent is often intended to provide a means of legal protection for the institution rather than to inform the consumer.[20] Many institutions recognize the need for and benefits of educating the public about privacy rights and obligations. Some distribute brochures while others impart information through television, radio, newspapers, and magazines, or by providing information to the public on request. These media provide the opportunity for institutions and organizations to educate the public about health information including:

- what personal information must legally be disclosed and when, how and what information is used and maintained, who will be given access to that data and under what conditions data will be released;

- how best to query an organization on the data being collected and maintained, how to access personal health records, and what rights an individual has with respect to disclosure and access;

- the responsibilities and expectations of both the data collector and the person about whom data are being collected as well as the legal implications of the informed consent form; and

- legal and governmental steps an individual can pursue when personal injury is incurred or when data are disclosed without permission, as well as penalties for breaches of confidentiality and improper disclosure of personal data.

Public education programs are usually available to those using clinics, hospitals, physician offices and other private sector places where health care services are provided. The public may also receive education about their rights and responsibilities regarding their personal information from organizations that compile, maintain, and share information, such as insurance companies, researchers, pharmaceutical companies, pharmacies, and health care equipment and services marketing companies.

The **United States Office of Consumer Affairs** sponsors many consumer education programs, conferences and seminars, and popular media campaigns and distributes brochures and leaflets. The Office is actively involved in policy making and has worked to have the Fair Credit Reporting Act amended to include provisions guaranteeing that the public receives education about how the credit reporting system works.

The **National Association of Insurance Commissioners's (NAIC)** model privacy bill requires insurance companies to, among other things, "...communicate to all agents and employees the responsibilities of handling confidential information;. .." and "... allow individuals to find out what information is contained in their personal insurance record, how it is being used and have an opportunity to amend their records to reflect their version in the event of a disputed fact. "[21] Although the bill has only been adopted by two States, it sends a clear signal that the insurance industry recognizes the importance of education and training programs. [22]

**AHIMA** has also published a brochure written specifically for the general public entitled "Your Health Information Belongs to You." This brochure contains simple terminology and discusses what a health record comprises, who owns the record, how a person can access his or her record and what information must be provided when doing so, what State laws govern records, and issues related to keeping a personal record at home.[23]

The **Privacy Rights Clearinghouse,** located in San Diego, California, is a nonprofit organization administered by the University of San Diego School of Law's Center for Public Interest Law and funded by a grant from the Telecommunication Education Trust. The Clearinghouse provides, free of charge, bilingual fact sheets to California consumers concerning, among other things, medical records. Its mission is to provide an up to date source of information on telecommunications related privacy issues for California consumers. In completing its mission, the Clearinghouse collects data on privacy abuses and informs consumers about their privacy rights and options.[24]

**The American Civil Liberties Union (ACLU)** has supported public education through policy making efforts and general discussions. It has established the Privacy and Technology Project which serves as the "central public education and advocacy project," assessing new technologies and their effects on personal privacy; heightening the awareness of industry, media, and the public; and developing policy reforms and challenging proposals the ACLU believes are threatening to privacy civil rights. Additionally, the ACLU represents the public interest at Federal and State legislative hearings, policy drafting sessions, judicial hearings, press/media occasions and conferences and workshops."

The **Canadian government** has taken a proactive approach to educating its citizenry and has placed the responsibility for educating the public and employees about privacy and confidentiality with respect to health information under the auspices of both the national and provincial governments. The **Office of the Privacy Commissioner of Canada** is responsible for privacy at the national level. All of the provinces have an obligation to educate the public on the handling of personal information, including health information, and share a corm-non goal of highlighting public awareness.

While each province has an information and privacy Commission, each differs somewhat in their particular laws.[26] As an example, the government of **Ontario** educates and disseminates information to their residents through speaking engagements, free newsletters, libraries and local media. The **Office of the Information and Privacy Commissioner** publishes a number of informational materials. *IPC* Perspectives is intended to provide helpful, practical information that is clearly expressed and easy to read. It is published three times a year in French and English.[27]

**Quebec** has recently enacted a new **Civil Code** that sets out rights for the protection of personal information and a new Act entitled "An Act Respecting the Protection of Personal Information in the Private Sector" which establishes rules for the exercise of those rights. The Act regulates how and when personal information can be collected, held, used or disclosed in the course of running a business in Quebec. The new Civil Code and the new Act, which became effective January 19, 1994, applies to health information and extends privacy protection to the private sector in the province of Quebec.[28] It is the first legislation in North America to regulate private sector collection, use, and disclosure of client and employee personal data.

***SUMMARY***

Some institutions and organizations have taken it upon themselves to educate their employees and consumers. Health care providers, organizations, and institutions that use health data and consumer based organizations have implemented training and education programs. These entities have found that the costs of such training programs are outweighed by the benefits of well informed and trained employees and educated consumers who are cognizant of their rights. Education for the public and appropriate employees, whether provided by an institution, a State, or the Federal government, will help ensure that all concerned parties

understand the possible ramifications of releasing health information maintained on individuals and the importance of confidentiality. Training the public and appropriate employees will help to put into action and make effective privacy regulations and security standards developed to protect personal data.

## *ENDNOTES*


1. Sullivan RL, Wircenski JL, Arnold SS, Sarkees MD. The ***Trainer's Guide: A Practical Manual for the Design Delivery and Evaluation of Training.*** Rockville, MD: Aspen Publishers, Inc. 1990.

***2.*** Patient education as a part of informed consent was discussed by the American Medical Association, American Hospital Association, and American Medical Record Association/American Health Information Management Association in their presentations to the DHHS Privacy Task Force.

*3.* Faden R, Beauchamp T. ***A History and Theory*** **of** ***Informed Consent, New*** York: Oxford University Press. 1986.

***4. See:*** Medical Information Bureau, Inc. ***A Consumer's Guide to the Medical Information Bureau.*** Westwood, **MA: Author. 1992; Medical Information Bureau, Inc.** ***The Consumer's MIB Fact Sheet.*** Westwood, MA: Author. 1992.; and Christie L. ***Health Data and the Private Sector.*** Presented at the DHHS Task Force on Privacy conference, "Health Records: Social Needs and Personal Privacy;" February 11, 1993; Washington, DC.

*5.* Smith RE. ***The Privacy Journal.*** Providence, RI: Privacy Journal; and Hendricks E. ***Privacy Times.*** Washington, DC: Privacy Times.

6. Sullivan. 1990.

***7.*** Written testimony of the American Nurses Association to the DHHS Task Force on Privacy. Washington, DC. October 13, 1992:6.

8. Amatayukl M. Presentation to the DHHS Task Force on Privacy. Washington, DC. March 26, 1992.

9. American Medical Record Association. ***Confidentiality of Patient Health Information.*** Chicago, IL: Author. 1985.

10. The American Dental Association. ***Principles of Ethics and Code of Professional Conduct.*** Washington, DC: Author. Revised January 1993.

11. American Hospital Association. ***Institutional Policies for Disclosure of Medical Record Information.*** Chicago, IL: Author. 1979.

***12. Model State Legislation on Confidentiality of Health Care Information,*** originally approved by the American Medical Association House of Delegates in June 1976 and revised by the House of Delegates in December 1981.

**13. American Nurses Association. 1992.**

14. American Pharmaceutical Association. The ***American Pharmaceutical Association Code of Ethics.*** Washington, DC: Author. 1981. Revised Ed.

15. American Psychiatry Association Committee on Confidentiality. ***American Journal of Psychiatry.*** Washington, DC: APA. November 1987; 144: 11.

16. Society of Consumer Affairs Professionals. ***Consumer Education and Information.*** American Express. 1982.

17. American Medical Record Association. ***Confidentiality of Patient Health Information, A Position Statement of the American Medical Record Association.*** Chicago, IL: Author. 1985. A revision of this statement is currently being made according to staff of the American Health Information Management Association.

18. Christie L. ***Health Data and the Private Sector.*** Presented at the DHHS Task Force on Privacy Conference, Health Records: Social Needs and Personal Privacy. Washington, DC. February 11, 1993.

19. Medical Information Bureau, Inc. ***The Consumer's MIB Fact Sheet.*** Westwood, MA: Author. 1992; and Day N. Presentation to the DHHS Task Force on Privacy. Washington, DC. August 25, 1992.

***20.*** Faden R, Geller G, Powers M, eds. ***AIDS, Women, and the Next Generation. New*** York: Oxford University Press. 1991.

21. Statement from the American Council of Life Insurance provided to the DHHS Privacy Task Force entitled ***Privacy and Confidentiality Standards in the Life and Health Insurance Business. 1992.***

22. Meletzke 0. Presentation to the DHHS Task Force on Privacy of Medical Records. Washington, DC. October 13, 1992.

***23.*** American Health Information Management Association, Professional Practice Division. ***Your Health Information Belongs to You.*** Chicago, IL: Author. March 1992.

***24.*** Center for Public Interest Law. ***Privacy Rights Clearinghouse.*** San Diego, CA: University of San Diego School of Law. 1992. Flyer on services offered which includes fact sheets, bilingual, on privacy issues, with toll free number for questions.

25. Letter to Hilary Clinton dated March 2, 1993, signed by Laura Murphy Lee, Director ACLU Washington Office and Janlori Goldman, ACLU Privacy and Technology Project. Ms. Goldman recently left the ACLU to take a position as Director of the Privacy and Technology Project for the Electronic Frontier Foundation. The project is focusing on privacy and technology as the electronic frontier is developed.

26. Canadian Privacy Commissioner. ***Annual Report Privacy Commissioner 1992-1993 of Canada.*** Ottawa, Ontario: Canada Communication Group. 1993:37.

27. ***IPC Perspectives.*** Ontario, Canada: Office of Information and Privacy Commissioner of Ontario. Spring 1993;2(2). Discussions held with Mr. Paul-Andre Comeau, Chairman, Office of Information and Privacy of Quebec and Ms. Ann Cavoukian, Ph.D., Assistant Commissioner, Office of the Information and Privacy Commissioner of Ontario.

28. Canadian Privacy Commissioner. 1993:37.

# Appendix A:

Mission Statement,
Questions to be Addressed by the Task Force,
Task Force Activities,
and
Lists of Presenters to the Privacy Task Force and
Conference Speakers

**TASK FORCE ON THE PRIVACY OF PRIVATE-SECTOR HEALTH RECORDS**
**ORIGINAL MISSION STATEMENT**

## *Task Force Mandate*

The HHS Task Force on the Privacy of Private-Sector Health Records will examine the extent to which a problem exists regarding use of personally identifiable records by doctors, hospitals, laboratories, pharmacies, insurance companies, medical information bureaus, and other private organizations in the absence of a federal policy to protect individuals from invasions of their privacy. The task force also will review current State laws on the privacy of medical records and the status of the recommendations of the Privacy Protection Study Commission of the early 1970s concerning the privacy of these records. The task force will consider steps that the federal government could appropriately pursue to protect these nonfederal record systems. Considerations may range from maintaining the status quo to consumer education, proposals for legislation, model State laws, and the strengthening of existing mechanisms for the protection of medical and other health records. At the same, the Task Force must be responsive to legitimate needs for information in the public and private sectors.

In April 1990, Assistant Secretary for Planning and Evaluation Martin H. Gerry established this interdepartmental task force.

Task force members represent the following operating and staff divisions within the department: Administration for Children and Families, Health Care Financing Administration, Public Health Service, Social Security Administration, Office of the Assistant Secretary for Management and Budget, Office of the Assistant Secretary for Planning and Evaluation, Office of the Assistant Secretary for Public Affairs, and Office of the General Counsel. Dr. Joan Turek-Brezina, Director, Technical and Computer Support (ASPE), serves as chair.

## *Task Force Activities*

To accomplish its mission, the task force has thus far identified the following activities.

- Identify existing private-sector policies and procedures for collecting, using, and disseminating personally identifiable health data as well as policies and procedures that may be adopted in the near future.

Identify the types of private-sector organizations that collect, use, and/or disseminate personally identifiable health data (e.g., researchers, direct marketing companies, insurance providers, employers).

Identify the type of data being collected, used, and disseminated.

Identify the most common methods of data collection.

Identify existing policies and procedures for discovering and correcting inaccurate data resulting from unintentional causes (e.g., mistaken entry, negligence) and existing policies and procedures for addressing the consequences of inaccurate data (e.g., Who pays to correct the error?).

Analyze reasons personally identifiable health data are being collected, used, and disseminated.

Identify existing policies and procedures for preventing, discovering, and correcting intentional misuse of data (e.g., computer security, theft, statistical manipulation).

Analyze reasons personally identifiable health data are being collected, used, and disseminated.

Identify the principles that govern decision making by private-sector organizations and individuals when determining if an individual's right to privacy should be compromised (e.g., when the health-care provider becomes aware that a patient poses a life-threat to another individual).

Analyze why existing privacy policies and procedures have been adopted and why other policies and procedures have been considered but rejected (e.g., cost, individual's rights considered more important than society's rights).

- Identify existing privacy problems related to collecting, using, and disseminating personally identifiable health data as well as problems that may arise in the near future (e.g., developing trends in computer technology, marketing, or health-care record keeping).

Identify affected populations.

Identify severity of each problem.

Identify frequency of occurrence of each problem.

Identify the facility with which each problem can be corrected.

- Identify the role ethics, regulation, and legislation have played in the development of existing privacy policies, procedures, and problems as well as the role they could play in establishing future policies and procedures and in preventing future problems.
- Identify State and local legislation or case law relating to private-sector collection, use, and/or dissemination of personally identifiable health data.
- Identify existing consumer-education programs that help make the public aware of the ways in which health data are being collected, used, and disseminated and the recourse the public can take if desired.

## QUESTIONS TO BE ADDRESSED BY THE TASK FORCE

**In an effort to consider steps that the Federal government could appropriately take to protect private sector health records, the members of the Task Force on the Privacy of Private-Sector Health Records have identified the following questions which they feel they must answer:**

What constitutes a health record?

What information is collected?

Who collects the information?

How is information entered, stored, retrieved?

For what reason is the information collected?

How is the record used?

Is the record a primary or secondary one?

Who owns the record?

Can the individual see his/her own record?

Who is responsible for inaccuracies in the record?

Who can change or correct the record? When a record is changed or corrected, are there (or should there be) standard procedures for bringing the corrected information to the attention of persons to whom the record had been previously disclosed?

When an individual is asked to provide information that will be put into a health record, what is he/she told about how the information is expected to be used and to whom it may be disclosed?

To whom is the record made available? To what extent is the individual's consent sought when a record is to be disclosed or turned over to another agency or organization, especially when time has elapsed since the individual's interaction with the health care related system?

What is the mode of sharing the record?

Does the record contain personal identifiers? What constitutes personal identifiers? When the record is shared, are personal identifiers included?

Can the health record be linked to other kinds of records, and under what conditions? What precautions are being taken, or can be taken, to prevent record linkage?

Should specially sensitive records be protected by special precautions/procedures?

What privacy and confidentiality laws (Federal, State, local) and industry and/or professional standards control collection, use, access to data?

What self imposed privacy and confidentiality rules control collection, use, access to data? Describe how these rules are enforced, what kinds of sanctions have actually been imposed, and how frequently they have been imposed?

What is the public perception of privacy? Personal privacy rights? Current privacy laws and their effectiveness?

What is the impact of the automation of health related records on the privacy and confidentiality of private sector health records?

What is a data protection board? Is it feasible and suggested for the U.S.?

# TASK FORCE ACTIVITIES

To accomplish its mission, the Task Force identified and completed the following activities:

Identified existing private-sector policies and procedures for collecting, using, and disseminating personally identifiable health data as well as policies and procedures that may be adopted in the near future.

- *Identified* ***the types of private-sector organizations that collect, use and/or disseminate personally identifiable health data (e.g., researchers, direct marketing companies, insurance providers, employers).***
- ***Identtjied the types of data being collected, used, and disseminated.***
- ***Identified the most common methods of data collection.***
- ***Identtjied existing policies and procedures for discovering and correcting inaccurate data resulting from unintentional causes (e.g., mistaken entry, negligence) and existing policies and procedures for addressing the consequences of inaccurate data (e.g., Who pays to correct the error?).***
- ***Identified existing policies and procedures for preventing, discovering, and correcting intentionally misuse of data (e.g., computer security, theft, statistical manipulation).***
- ***Analyzed reasons personally identifiable health data are being collected, used, and disseminated.***
- ***Identified the factors that govern decision making by private-sector organizations and individuals when determining if an individuals right to privacy should be compromised (e.g., when the health care provider becomes aware that a patient poses a life-threat to another individual).***
- ***Analyzed why existing privacy policies and procedures have been adopted and why other policies and procedures have been considered but rejected (e.g., cost of implementation, individuals rights considered more important than society's rights).***

Identified existing privacy problems related to collecting, using, and disseminating personally identifiable health data as well as problems that may arise in the near future (e.g., developing trends in computer technology, marketing, or health care record keeping).

- *Identijied affected populations.*
- *Identijied the severity of each problem.*
- *Identified frequency of occurrence of each problem.*
- *Identify the facility with which each problem can be corrected.*

Identified the role ethics, regulation, and legislation have played in the development of existing privacy policies, procedures, and problems as well as the role they could play in establishing future policies and procedures and in preventing future problems.

Identified State and local legislation or case law relating to private sector collection, use and/or dissemination of personally identifiable health data.

Identified existing consumer-education programs that help make the public aware of the ways in which health data are being collected, used, and disseminated and the recourse the public can take if desired.

| PRESENTERS TO THE PRIVACY TASK FORCE | | |
|---|---|---|
| Stakeholder Category | Name/Association | Topic/Date |
| Privacy Advocates | Evan Hendricks<br>Editor, Privacy Times | Current and Future Privacy Needs, 1/28/92 |
| | Marc Rotenburg<br>Director, Washington Office, CPSR | Current and Future Privacy Needs, 2/18/92 |
| | Michele Zavos<br>AIDS Coordinating Project, ABA | Special Circumstances and Privacy Needs, 2/25/92 |
| | Peter Hawley, MD<br>Medical Director, Whitman Walker Clinic | Special Circumstances and Privacy Needs, 2/25/92 |
| | William Pierce, Mary Beth Seader<br>National Committee for Adoption | Adoption Records and Privacy, 9/15/92 |
| Technological Arena | Vincent Brannigan<br>Professor, University of Maryland | Technology and Confidentiality, International Aspects of Privacy, 1/28/92 |
| | Dr. Berndt Beier,<br>Germany | International Privacy Guidelines and Technological Developments, 7/14/92 |
| Legal Arena | Ron Plesser<br>Attorney, Piper & Marbury | Privacy Legislation, 2/18/92 |
| | Robert Gellman<br>Chief Counsel, Subcommittee on Government Information, Justice & Agriculture | The Data Protection Board Bill and Privacy Protection Needs of Genetic Information, 5/26/92 |
| Professional Organizations | Margret Amatayakul,<br>lnterim Executive Director, CPRI | Privacy and the Computer-based Patient Record, 3/24/9 1 |
| | Betty Fuchs<br>Project Director, JCAHO | JCAHO and Privacy Concerns in Hospitals and Patient Records, 4/14/92 |
| | Donna Pickett<br>American Hospital Association | AHA's Position on Privacy and Confidentiality, Submitted written testimony |
| | American Dental Association | Dentistry and Privacy Concerns, Submitting written testimony |
| | Dr. Barbara Heller,<br>American Nurses Association | Nursing and Privacy Concerns, Submitted written testimony |
| | American Pharmaceutical Association | Pharmaceutical Records and Confidentiality, Submitting written testimony |
| | E. Harvey Estes<br>Ethics and Health Policy Council, AMA | AMA, Physicians, Patient Records, and Privacy, 1 1/10/92 |

| | | |
|---|---|---|
| Data Management Arena | Mark Epstein, Sc.D.<br>Executive Director, NAHDO | Privacy, Confidentiality, and Health Data Collection/Databanks, 10/27/92 |
| | Rosanna Coffey,<br>Director, Division of Provider Studies, AHCPR | Privacy, Research, and Databases, 10/27/92 |
| | Elliott Stone<br>Executive Director, MA Health Data Consortium | Privacy and Data Collection, 9/15/92 |
| | Peter Waegemann<br>Executive Director, Medical Records Institute | Medical Records and the Lessons Learned from Europe, 9/29/92 |
| | Neil Day, President<br>Medical Information Bureau | The MIB, stored information, and privacy, 8/25/92 |
| Vendor Arena | Andrew Garling, MD<br>TDS | Changing Privacy Needs and Technological Developments, 7/14/92 |
| | John Morgan, Ph.D.<br>3M Health Care Systems | Changing Privacy Needs in Response to Developing Technology, 4/14/92 |
| Insurance Arena | Otto Meletzke<br>Senior Council, American Council of Life Insurance | Insurance, Privacy Protection Act, and Data Collection, 10/13/92 |
| Credit Arena | John Baker<br>Senior Vice President, Equifax | Privacy, Confidentiality, and Credit, 6/9/92 |
| Media Arena | Paul McMasters<br>Vice President, Freedom Forum | Privacy, Public Information, and the Media, 5/26/92 |
| Other Privacy Efforts | Kathy Lohr, Ph.D.<br>Deputy Director, Health Care Services, Institute of Medicine | Privacy Concerns with Regional Health Databanks, 4/28/92 |

| PRIVACY CONFERENCE SPEAKERS BY CATEGORY | | |
|---|---|---|
| Stakeholder Category | Name/Association | Topic/Date |
| Privacy Advocates | Michael Yesley, J.D.<br>Los Alamos National Laboratory | Consequences to the individual of data collection and information use |
| | Larry Gosten, J.D.<br>American Society of Law and Medicine | Individual expectations and societal needs |
| Technological Arena | Vincent Brannigan, J.D.<br>Professor, University of Maryland | Ownership, Uses, and Dissemination of Electronic Health Care Information |
| | Michael Fitzrnaurice, Ph.D.<br>Director, OSDD, AHCPR | Ownership, Uses, and Dissemination of Electronic Health Care Information |
| Research Arena | David Pryor, M.D.<br>Duke University | Research Use of Health Records |
| | Dale Schumacher, M.D., M.Ed., M.P.H.<br>Commission for Professional and Hospital Activities | Research Use of Health Records |
| Private Sector | Willis Ware, Ph.D.<br>RAND Corporation | Lessons for the Future |
| | Florence Rice,<br>Harlem Consumer Education Council | Monitoring, surveillance and law enforcement |
| a Management Arena | Peter Waegemann<br>Executive Director, Medical Records Institute | |
| | Janice Curtis, M.S.P.H.<br>Duke University | Administrative and State Uses for Health Data |
| Marketing Arena | Lorna Christie<br>Direct Marketer's Association | Health Data and the Private Sector |
| Academic Arena | Ruth Faden, Ph.D.<br>Johns Hopkins University | Maintaining the Balance between Privacy and Informational Need |
| | David Flaherty, Ph.D.<br>University of Ontario | Conference Synopsis and Future Directions |
| | Madison Power, Ph.D.<br>Kennedy School of Ethics | Approaches to Privacy and Confidentiality Protection |
| Federal Sector | John Fanning, LL.B.<br>Privacy Task Force/Privacy Study Commission | Approaches to privacy and Confidentiality Protection |
| Other Privacy Efforts | Roger Bulger, M.D.<br>Institute of Medicine | Providers use of data |